

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日 2 0 0 2 年 1 0 月 1 1 日
Date of Application:

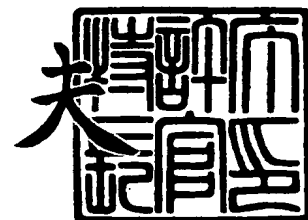
出 願 番 号 特 願 2 0 0 2 - 2 9 9 7 1 2
Application Number:
[ST. 10/C] : [J P 2 0 0 2 - 2 9 9 7 1 2]

出 願 人 株式会社リコー
Applicant(s):

2 0 0 3 年 8 月 2 7 日

特許庁長官
Commissioner,
Japan Patent Office

今 井 康 夫



【書類名】 特許願

【整理番号】 0206313

【提出日】 平成14年10月11日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 12/00

【発明の名称】 ドキュメントファイルの印刷制御方法、ドキュメントファイル印刷制御システム、ドキュメントファイル印刷制御プログラム、ドキュメントファイル保護方法、ドキュメントファイル印刷方法、ドキュメントファイル保護プログラム、ドキュメントファイル印刷プログラム及びコンピュータ装置

【請求項の数】 23

【発明者】

【住所又は居所】 東京都大田区中馬込 1 丁目 3 番 6 号
株式会社リコー内

【氏名】 金井 洋一

【特許出願人】

【識別番号】 000006747

【氏名又は名称】 株式会社リコー

【代表者】 桜井 正光

【代理人】

【識別番号】 100084250

【弁理士】

【氏名又は名称】 丸山 隆夫

【電話番号】 03-3590-8902

【手数料の表示】

【予納台帳番号】 007250

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 0207936

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 ドキュメントファイルの印刷制御方法、ドキュメントファイル印刷制御システム、ドキュメントファイル印刷制御プログラム、ドキュメントファイル保護方法、ドキュメントファイル印刷方法、ドキュメントファイル保護プログラム、ドキュメントファイル印刷プログラム及びコンピュータ装置

【特許請求の範囲】

【請求項 1】 ドキュメントファイルに、該ドキュメントファイルの印刷要件を示す印刷制御情報を付与し、

前記印刷要件を満たすことなく前記ドキュメントファイルを印刷することを禁止することにより該ドキュメントファイルを保護し、

保護したドキュメントファイルを印刷する際に、前記印刷要件を満たすように印刷処理を行うドキュメントの印刷制御方法。

【請求項 2】 ドキュメントファイルに、該ドキュメントファイルの印刷要件を示す印刷制御情報を付与し、

前記印刷要件を満たすことなく前記ドキュメントファイルを印刷することを、ユーザの秘密コードを用いて禁止することにより該ドキュメントファイルを保護し、

前記ユーザの秘密コードが得られた場合にのみ、前記保護したドキュメントファイルの印刷を許可し、

保護したドキュメントファイルを印刷する際に、前記印刷要件を満たすように印刷処理を行うドキュメントファイルの印刷制御方法。

【請求項 3】 ドキュメントファイルに、ユーザごとに設定された該ドキュメントファイルのアクセス要件を示すアクセス制御情報を関連づけ、

該アクセス制御情報によって示されるアクセス要件を満たすことなく前記ドキュメントファイルを印刷することを禁止することにより該ドキュメントファイルを保護し、

保護したドキュメントファイルにアクセスする際に、前記アクセス要件を満足させ、

前記ドキュメントファイルを印刷する際の要件が、前記アクセス要件に含まれ

るドキュメントファイルの印刷制御方法。

【請求項 4】 ドキュメントファイルを、セキュリティポリシーに対応するとともに該ドキュメントファイルのアクセス要件を示すセキュリティ属性と関連づけ、

前記セキュリティポリシーに従うことなく前記ドキュメントファイルへアクセスすることを禁止することにより該ドキュメントファイルを保護し、

保護したドキュメントファイルに対するアクセスを、前記セキュリティ属性に基づくとともに前記セキュリティポリシーに従って制御し、

前記セキュリティポリシーに、前記ドキュメントファイルを印刷する際の要件が含まれるドキュメントファイルの印刷制御方法。

【請求項 5】 前記ドキュメントファイルがポータブルドキュメントファイルであることを特徴とする請求項 1 から 4 のいずれか 1 項記載のドキュメントファイルの印刷制御方法。

【請求項 6】 ドキュメントファイルに、該ドキュメントファイルの印刷要件を示す印刷制御情報を付与する手段と、

前記印刷要件を満たすことなく前記ドキュメントファイルを印刷することを禁止することにより該ドキュメントファイルを保護する手段と、

保護したドキュメントファイルを印刷する際に、前記印刷要件を満たすように印刷処理を行う手段とを有するドキュメント印刷制御システム。

【請求項 7】 ドキュメントファイルに、該ドキュメントファイルの印刷要件を示す印刷制御情報を付与する手段と、

前記印刷要件を満たすことなく前記ドキュメントファイルを印刷することを、ユーザの秘密コードを用いて禁止することにより該ドキュメントファイルを保護する手段と、

前記ユーザの秘密コードが得られた場合にのみ、前記保護したドキュメントファイルの印刷を許可する手段と、

保護したドキュメントファイルを印刷する際に、前記印刷要件を満たすように印刷処理を行う手段とを有するドキュメントファイル印刷制御システム。

【請求項 8】 ドキュメントファイルに、ユーザごとに設定された該ドキュ

メントファイルのアクセス要件を示すアクセス制御情報を関連づける手段と、

該アクセス制御情報によって示されるアクセス要件を満たすことなく前記ドキュメントファイルを印刷することを禁止することにより該ドキュメントファイルを保護する手段と、

保護したドキュメントファイルにアクセスする際に、前記アクセス要件を満足させる手段とを有し、

前記ドキュメントファイルを印刷する際の要件が、前記アクセス要件に含まれて設定されたことを特徴とするドキュメントファイル印刷制御システム。

【請求項 9】 ドキュメントファイルを、セキュリティポリシーに対応するとともに該ドキュメントファイルのアクセス要件を示すセキュリティ属性と関連づける手段と、

前記セキュリティポリシーに従うことなく前記ドキュメントファイルへアクセスすることを禁止することにより該ドキュメントファイルを保護する手段と、

保護したドキュメントファイルに対するアクセスを、前記セキュリティ属性に基づくとともに前記セキュリティポリシーに従って制御する手段とを有し、

前記ドキュメントファイルを印刷する際の要件が、前記セキュリティポリシーに含まれて設定されたことを特徴とするドキュメントファイル印刷制御システム

。

【請求項 10】 前記ドキュメントファイルがポータブルドキュメントファイルであることを特徴とする請求項 6 から 9 のいずれか 1 項記載のドキュメントファイル印刷制御システム。

【請求項 11】 ドキュメントファイルに、該ドキュメントファイルの印刷要件を示す印刷制御情報を付与するステップと、

前記印刷要件を満たすことなく前記ドキュメントファイルを印刷することを禁止することにより該ドキュメントファイルを保護するステップと、

保護したドキュメントファイルを印刷する際に、前記印刷要件を満たすように印刷処理を実行するステップとを、コンピュータに実行させることを特徴とするドキュメント印刷制御プログラム。

【請求項 12】 ドキュメントファイルに、該ドキュメントファイルの印刷

要件を示す印刷制御情報を付与するステップと、

前記印刷要件を満たすことなく前記ドキュメントファイルを印刷することを、ユーザの秘密コードを用いて禁止することにより該ドキュメントファイルを保護するステップと、

前記ユーザの秘密コードが得られた場合にのみ、前記保護したドキュメントファイルの印刷を許可するステップと、

保護したドキュメントファイルを印刷する際に、前記印刷要件を満たすように印刷処理を行うステップとを、コンピュータに実行させることを特徴とするドキュメントファイル印刷制御プログラム。

【請求項 13】 ドキュメントファイルを印刷する際の要件を含んでユーザごとに設定された、該ドキュメントファイルのアクセス要件を示すアクセス制御情報を、前記ドキュメントファイルに関連づけるステップと、

該アクセス制御情報によって示されるアクセス要件を満たすことなく前記ドキュメントファイルを印刷することを禁止することにより該ドキュメントファイルを保護するステップと、

前記アクセス要件を満たしつつ、保護したドキュメントファイルにアクセスするステップとを、コンピュータに実行させることを特徴とするドキュメントファイル印刷制御プログラム。

【請求項 14】 セキュリティポリシーに対応するとともに、ドキュメントファイルを印刷する際の要件を含むアクセス要件を示すセキュリティ属性をドキュメントファイルに関連づけるステップと、

前記セキュリティポリシーに従うことなく前記ドキュメントファイルへアクセスすることを禁止することにより該ドキュメントファイルを保護するステップと

、
保護したドキュメントファイルに対するアクセスを、前記セキュリティ属性に基づくとともに前記セキュリティポリシーに従って制御するステップとをコンピュータに実行させることを特徴とするドキュメントファイル印刷制御プログラム。

【請求項 15】 前記ドキュメントファイルがポータブルドキュメントファ

イルであることを特徴とする請求項 1 1 から 1 4 のいずれか 1 項記載のドキュメントファイル印刷制御プログラム。

【請求項 1 6】 ドキュメントファイルに、該ドキュメントファイルの印刷要件を示す印刷制御情報を付与し、

前記印刷要件を満たしつつ前記ドキュメントファイルの印刷処理を行った場合にのみ、該ドキュメントファイルが印刷されるように保護して保護ドキュメントを生成することを特徴とするドキュメントファイル保護方法。

【請求項 1 7】 前記ドキュメントファイルがポータブルドキュメントファイルであることを特徴とする請求項 1 6 記載のドキュメントファイル保護方法。

【請求項 1 8】 請求項 1 6 又は 1 7 記載のドキュメントファイル保護方法によって生成された保護ドキュメントを印刷する方法であって、

前記保護ドキュメントに付与されている印刷制御情報を取得し、

該印刷制御情報を用いて印刷制御を行い、該印刷制御情報に示される印刷要件を満たしつつ前記保護ドキュメントを印刷することを特徴とするドキュメントファイル印刷方法。

【請求項 1 9】 ドキュメントファイルに、該ドキュメントファイルの印刷要件を示す印刷制御情報を付与するステップと、

前記印刷要件を満たしつつ前記ドキュメントファイルの印刷処理を行った場合にのみ、該ドキュメントファイルが印刷されるように保護して保護ドキュメントを生成するステップとをコンピュータに実行させることを特徴とするドキュメントファイル保護プログラム。

【請求項 2 0】 前記ドキュメントファイルがポータブルドキュメントファイルであることを特徴とする請求項 1 9 記載のドキュメントファイル保護プログラム。

【請求項 2 1】 請求項 1 6 若しくは 1 7 記載のドキュメント保護ファイル保護方法、又は請求項 1 9 若しくは 2 0 記載のドキュメント保護プログラムを実行するコンピュータによって生成された保護ドキュメントを印刷する処理をコンピュータに実行させるプログラムであって、

前記保護ドキュメントに付与されている印刷制御情報を取得するステップと、

該印刷制御情報を用いて印刷制御を行い、該印刷制御情報に示される印刷要件を満たしつつ前記保護ドキュメントを印刷するステップとをコンピュータに実行させることを特徴とするドキュメントファイル印刷プログラム。

【請求項 22】 請求項 19 又は 20 記載のドキュメントファイル保護プログラムを実行するコンピュータ装置。

【請求項 23】 請求項 21 記載のドキュメントファイル印刷プログラムを実行するコンピュータ装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、ドキュメントの漏洩を防止するためのドキュメントファイルの印刷制御方法、ドキュメントファイル印刷制御システム、ドキュメントファイル印刷制御プログラム、ドキュメントファイル保護方法、ドキュメントファイル印刷方法、ドキュメントファイル保護プログラム、ドキュメントファイル印刷プログラム及びコンピュータ装置に関し、特に、ドキュメントのプリントアウトからの情報の漏洩を防止するドキュメントファイルの印刷制御方法、ドキュメントファイル印刷制御システム、ドキュメントファイル印刷制御プログラム、ドキュメントファイル保護方法、ドキュメントファイル印刷方法、ドキュメントファイル保護プログラム、ドキュメントファイル印刷プログラム及びコンピュータ装置に関する。

【0002】

【従来の技術】

近年、文書や画像などの情報（以下、ドキュメントという）を取り扱うオフィスなどにおいては、ドキュメントを紙に印刷する代わりにドキュメントファイルとして情報記録媒体へ電子的に記録しておく手法が主流となっている。

【0003】

ドキュメントを電子的に記録すれば、紙資源を用いることなくドキュメントを記録できるため、省資源化を図れるとともに、ドキュメントが印刷された紙を格納する必要がなくなり、省スペース化を実現できる。

【0004】

また、ドキュメントを電子的に記録すれば、同一のドキュメントを多数人に対して同時に配布したり、遠隔地にいる者へネットワーク網を介してドキュメントを配布したりすることが可能となり、業務の効率化を図ることができる。

【0005】

同一のドキュメントを多数人に対して同時に配布したり、遠隔地にいる者へネットワーク網を介してドキュメントを配布できるというドキュメントを電子的に記録する場合の長所は、ドキュメントが漏洩しやすくなるという問題の裏返しでもある。

オフィスなどにおいて取り扱われるドキュメントの中には、機密性を要するものも多数存在するため、ドキュメントの漏洩を防止するための対策を講じる必要がある。

【0006】

ドキュメントの漏洩を防止することを目的とした従来技術としては、特許文献1に開示される「Method of encrypting information for remote access while maintaining access control」、特許文献2に開示される「Information security architecture for encrypting documents for remote access while maintaining access control」、及び、特許文献3に開示される「文書管理システム」のように、ドキュメントファイルを開く際にユーザ認証を求めて、正当なユーザだけがドキュメントの内容を参照できるようにする手法や、開いたドキュメントファイルを印刷しようとする際にユーザに印刷する権限があるか否かをチェックして権限があるユーザにのみ印刷させるものがある。

【0007】

また、特許文献4に開示される「電子的に伝送された情報の印刷制限方法および印刷制限付き文書」のように、支払いを済ませた場合にのみ印刷が許可されるようにドキュメントファイルをコントロールするような技術もある。

【0008】

【特許文献1】

米国特許第6339825号明細書

【特許文献 2】

米国特許第 6 2 8 9 4 5 0 号明細書

【特許文献 3】

特開 2 0 0 1 - 1 4 2 8 7 4 号公報

【特許文献 4】

特開 2 0 0 2 - 0 2 4 0 9 7 号公報

【0 0 0 9】**【発明が解決しようとする課題】**

上記各特許文献に開示される発明では、ユーザの権限に関わらず印刷が禁止された状態でドキュメントファイルを配布することとなるが、この場合は印刷に際して印刷が可能な状態に復元させなければならなくなるため、ドキュメントファイルの使い勝手が悪くなってしまう。よって、セキュリティが確保できるのであれば印刷が許可された状態でドキュメントファイルが配布することが好ましい。

【0 0 1 0】

また、上記各特許文献に開示される発明においては、権限のない者がドキュメントを印刷できないように設定できるものの、印刷した物（プリントアウト）に対するセキュリティは何ら設定されていない。

【0 0 1 1】

よって、印刷する権限を有するユーザになりすまして一度ドキュメントを印刷してしまえば、その後は何の制約を受けることなくドキュメントのプリントアウトを複製して他者に配布できることになる。

さらに、ドキュメントを漏洩させようとする者が印刷する権限を有する正当なユーザである場合は、これを阻止することはできない。

【0 0 1 2】

このように、従来の技術では、ドキュメントファイルの使い勝手が良くないとともに、プリントアウトによるドキュメントの漏洩を防止するためのセキュリティが不十分であるという問題があった。

【0 0 1 3】

本発明はかかる問題に鑑みてなされたものであり、ユーザの権限に応じたアク

セス制限を施した状態でドキュメントファイルを配布できるとともに、プリントアウトによるドキュメントの漏洩を防止したドキュメントファイルの印刷制御方法、ドキュメントファイル印刷制御システム、ドキュメントファイル印刷制御プログラム、ドキュメントファイル保護方法、ドキュメントファイル印刷方法、ドキュメントファイル保護プログラム、ドキュメントファイル印刷プログラム及びコンピュータ装置を提供することを目的とする。

【 0 0 1 4 】

【課題を解決するための手段】

上記目的を達成するため、本発明は、第 1 の態様として、ドキュメントのプリントアウトからの情報の漏洩を防止するドキュメントファイルの印刷制御方法を提供するものである。

本発明の第 1 の態様にかかる発明は、下記 1 - 1 から 1 - 4 のいずれかに示す方法である。

1 - 1 : ドキュメントファイルに、該ドキュメントファイルの印刷要件を示す印刷制御情報を付与し、印刷要件を満たすことなくドキュメントファイルを印刷することを禁止することにより該ドキュメントファイルを保護し、保護したドキュメントファイルを印刷する際に、印刷要件を満たすように印刷処理を行うドキュメントの印刷制御方法。

1 - 2 : ドキュメントファイルに、該ドキュメントファイルの印刷要件を示す印刷制御情報を付与し、印刷要件を満たすことなくドキュメントファイルを印刷することを、ユーザの秘密コードを用いて禁止することにより該ドキュメントファイルを保護し、ユーザの秘密コードが得られた場合にのみ、保護したドキュメントファイルの印刷を許可し、保護したドキュメントファイルを印刷する際に、印刷要件を満たすように印刷処理を行うドキュメントファイルの印刷制御方法。

1 - 3 : ドキュメントファイルに、ユーザごとに設定された該ドキュメントファイルのアクセス要件を示すアクセス制御情報を関連づけ、該アクセス制御情報によって示されるアクセス要件を満たすことなくドキュメントファイルを印刷することを禁止することにより該ドキュメントファイルを保護し、保護したドキュメントファイルにアクセスする際に、アクセス要件を満足させ、ドキュメントフ

ファイルを印刷する際の要件が、アクセス要件に含まれるドキュメントファイルの印刷制御方法。

1-4：ドキュメントファイルを、セキュリティポリシーに対応するとともに該ドキュメントファイルのアクセス要件を示すセキュリティ属性と関連づけ、セキュリティポリシーに従うことなくドキュメントファイルへアクセスすることを禁止することにより該ドキュメントファイルを保護し、保護したドキュメントファイルに対するアクセスを、セキュリティ属性に基づくとともにセキュリティポリシーに従って制御し、セキュリティポリシーに、ドキュメントファイルを印刷する際の要件に含まれるドキュメントファイルの印刷制御方法。

【0015】

上記本発明の第1の態様において、ドキュメントファイルがポータブルドキュメントファイルであることが好ましい。

【0016】

また、上記目的を達成するため、本発明は、第2の態様として、ドキュメントのプリントアウトからの情報の漏洩を防止するドキュメントファイル印刷制御システムを提供するものである。

上記本発明の第2態様にかかる発明は、下記2-1から2-4のいずれかに示す構成である。

2-1：ドキュメントファイルに、該ドキュメントファイルの印刷要件を示す印刷制御情報を付与する手段と、印刷要件を満たすことなくドキュメントファイルを印刷することを禁止することにより該ドキュメントファイルを保護する手段と、保護したドキュメントファイルを印刷する際に、印刷要件を満たすように印刷処理を行う手段とを有するドキュメント印刷制御システム。

2-2：ドキュメントファイルに、該ドキュメントファイルの印刷要件を示す印刷制御情報を付与する手段と、印刷要件を満たすことなくドキュメントファイルを印刷することを、ユーザの秘密コードを用いて禁止することにより該ドキュメントファイルを保護する手段と、ユーザの秘密コードが得られた場合にのみ、保護したドキュメントファイルの印刷を許可する手段と、保護したドキュメントファイルを印刷する際に、印刷要件を満たすように印刷処理を行う手段とを有す

るドキュメントファイル印刷制御システム。

2-3：ドキュメントファイルに、ユーザごとに設定された該ドキュメントファイルのアクセス要件を示すアクセス制御情報を関連づける手段と、該アクセス制御情報によって示されるアクセス要件を満たすことなくドキュメントファイルを印刷することを禁止することにより該ドキュメントファイルを保護する手段と、保護したドキュメントファイルにアクセスする際に、アクセス要件を満足させる手段とを有し、ドキュメントファイルを印刷する際の要件が、アクセス要件に含まれて設定されたことを特徴とするドキュメントファイル印刷制御システム。

2-4：ドキュメントファイルを、セキュリティポリシーに対応するとともに該ドキュメントファイルのアクセス要件を示すセキュリティ属性と関連づける手段と、セキュリティポリシーに従うことなくドキュメントファイルへアクセスすることを禁止することにより該ドキュメントファイルを保護する手段と、保護したドキュメントファイルに対するアクセスを、セキュリティ属性に基づくとともにセキュリティポリシーに従って制御する手段とを有し、ドキュメントファイルを印刷する際の要件が、セキュリティポリシーに含まれて設定されたことを特徴とするドキュメントファイル印刷制御システム。

【0017】

上記本発明の第2の態様において、ドキュメントファイルはポータブルドキュメントファイルであることが好ましい。

【0018】

また、上記目的を達成するため、本発明は、第3の態様として、ドキュメントのプリントアウトからの情報の漏洩を防止するドキュメントファイルの印刷制御方法をコンピュータに実行させるドキュメントファイル印刷制御プログラムを提供するものである。

本発明の第3の態様にかかる発明は、下記3-1から3-4のいずれかに示すプログラムである。

3-1：ドキュメントファイルに、該ドキュメントファイルの印刷要件を示す印刷制御情報を付与するステップと、印刷要件を満たすことなくドキュメントファイルを印刷することを禁止することにより該ドキュメントファイルを保護する

ステップと、保護したドキュメントファイルを印刷する際に、印刷要件を満たすように印刷処理を実行するステップとを、コンピュータに実行させることを特徴とするドキュメント印刷制御プログラム。

3-2：ドキュメントファイルに、該ドキュメントファイルの印刷要件を示す印刷制御情報を付与するステップと、印刷要件を満たすことなくドキュメントファイルを印刷することを、ユーザの秘密コードを用いて禁止することにより該ドキュメントファイルを保護するステップと、ユーザの秘密コードが得られた場合にのみ、保護したドキュメントファイルの印刷を許可するステップと、保護したドキュメントファイルを印刷する際に、印刷要件を満たすように印刷処理を行うステップとを、コンピュータに実行させることを特徴とするドキュメントファイル印刷制御プログラム。

3-3：ドキュメントファイルを印刷する際の要件を含んでユーザごとに設定された、該ドキュメントファイルのアクセス要件を示すアクセス制御情報を、ドキュメントファイルに関連づけるステップと、該アクセス制御情報によって示されるアクセス要件を満たすことなくドキュメントファイルを印刷することを禁止することにより該ドキュメントファイルを保護するステップと、アクセス要件を満たしつつ、保護したドキュメントファイルにアクセスするステップとを、コンピュータに実行させることを特徴とするドキュメントファイル印刷制御プログラム。

3-4：セキュリティポリシーに対応するとともに、ドキュメントファイルを印刷する際の要件を含むアクセス要件を示すセキュリティ属性をドキュメントファイルに関連づけるステップと、セキュリティポリシーに従うことなくドキュメントファイルへアクセスすることを禁止することにより該ドキュメントファイルを保護するステップと、保護したドキュメントファイルに対するアクセスを、セキュリティ属性に基づくとともにセキュリティポリシーに従って制御するステップとをコンピュータに実行させることを特徴とするドキュメントファイル印刷制御プログラム。

【0019】

上記本発明の第3の態様において、ドキュメントファイルはポータブルドキュ

メントファイルであることが好ましい。

【0020】

また、上記目的を達成するため、本発明は第4の態様として、ドキュメントファイルに、該ドキュメントファイルの印刷要件を示す印刷制御情報を付与し、

印刷要件を満たしつつドキュメントファイルの印刷処理を行った場合にのみ、該ドキュメントファイルが印刷されるように保護して保護ドキュメントを生成することを特徴とするドキュメントファイル保護方法を提供するものである。

上記本発明の第4の態様において、ドキュメントファイルはポータブルドキュメントファイルであることが好ましい。

【0021】

また、上記目的を達成するため、本発明は、第5の態様として、上記本発明の第4の態様にかかるドキュメントファイル保護方法によって生成された保護ドキュメントを印刷する方法であって、保護ドキュメントに付与されている印刷制御情報を取得し、該印刷制御情報を用いて印刷制御を行い、該印刷制御情報に示される印刷要件を満たしつつ保護ドキュメントを印刷することを特徴とするドキュメントファイル印刷方法を提供するものである。

【0022】

また、上記目的を達成するため、本発明は、第6の態様として、ドキュメントファイルに、該ドキュメントファイルの印刷要件を示す印刷制御情報を付与するステップと、印刷要件を満たしつつドキュメントファイルの印刷処理を行った場合にのみ、該ドキュメントファイルが印刷されるように保護して保護ドキュメントを生成するステップとをコンピュータに実行させることを特徴とするドキュメントファイル保護プログラムを提供するものである。

上記本発明の第6の態様において、ドキュメントファイルはポータブルドキュメントファイルであることが好ましい。

【0023】

また、上記目的を達成するため、本発明は、第7の態様として、上記本発明の第4の態様にかかるドキュメントファイルの保護方法によって生成した保護ドキュメント、又は、コンピュータに上記本発明の第6の態様にかかるドキュメント

ファイル保護プログラムを実行させて生成した保護ドキュメントを印刷する処理をコンピュータに実行させるプログラムであって、保護ドキュメントに付与されている印刷制御情報を取得するステップと、該印刷制御情報を用いて印刷制御を行い、該印刷制御情報に示される印刷要件を満たしつつ保護ドキュメントを印刷するステップとをコンピュータに実行させることを特徴とするドキュメントファイル印刷プログラムを提供するものである。

【0024】

また、上記目的を達成するため、本発明は、第8の態様として、上記本発明の第6の態様にかかるドキュメントファイル保護プログラムを実行するコンピュータ装置を提供するものである。

【0025】

また、上記目的を達成するため、本発明は、第9の態様として、上記本発明の第7の態様にかかるドキュメントファイル印刷プログラムを実行するコンピュータ装置を提供するものである。

【0026】

〔作用〕

本発明によれば、ドキュメントファイルを配布する者が、ドキュメントファイルのセキュリティ及びドキュメントのプリントアウトのセキュリティを確保するための処理を設定し、その処理を印刷時に強制できる。

【0027】

【発明の実施の形態】

〔第1の実施形態〕

本発明を好適に実施した第1の実施形態について説明する。

図1に、本実施形態にかかるドキュメント保護・印刷システムの構成を示す。

本実施形態にかかるドキュメント保護・印刷システムは、配布者端末101とユーザ端末102とプリンタ103とを有する。配布者端末101及びユーザ端末102は、表示装置（例えば、LCD）、入力装置（例えば、キーボード）、外部記録装置（例えば、FDD、HDD）などを備えたコンピュータ端末を適用できる。なお、配布者端末101にはドキュメント保護プログラム111が、ユ

ーザ端末 1 0 2 にはドキュメント印刷プログラム 1 2 1 がそれぞれ実装されている。

【 0 0 2 8 】

ドキュメント保護プログラム 1 1 1 は、ドキュメントファイルに配布者端末 1 0 1 の使用者（以下、配布者という）の入力操作に応じて印刷要件を設定するとともに、暗号化アルゴリズム（RC4、Triple DES、IDEAなど）を用いてドキュメントファイルを暗号化し、保護ドキュメントを生成する処理を行うプログラムである。

【 0 0 2 9 】

ドキュメント印刷プログラム 1 2 1 は、ユーザ端末 1 0 2 の使用者（以下、ユーザという）の入力操作に応じ、保護ドキュメントを復号化するとともに設定されている印刷要件に応じた印刷処理をプリンタ 1 0 3 に実行させる処理を行うプログラムである。

【 0 0 3 0 】

なお、配布者の入力操作に応じてドキュメント保護プログラム 1 1 1 がドキュメントファイルに設定する印刷要件の一例としては、地紋印刷（Background Dot Pattern：以下、BDPという）、機密印刷（Private Access：以下、PACという）、電子透かし（Digital Watermark：以下、DWMという）の付加、バーコード付加（Embedding Barcode：以下、EBCという）、機密ラベルスタンプ（Security Label Stamp：以下、SLSという）などが挙げられる。

【 0 0 3 1 】

本実施形態にかかるドキュメント保護・印刷システムの動作について説明する。まず、システム全体の動作について説明する。

配布者は、配布者端末 1 0 1 を操作してこれにドキュメントファイルを実装しておく。例えば、入力装置を用いて配布者がドキュメントファイルを作成してもよいし、外部記録装置を用いて情報記録媒体に記録されたドキュメントファイルを読み取らせても良い。

【 0 0 3 2 】

ドキュメントファイルにセキュリティを設定する場合、配布者は配布者端末 1

01の入力装置を操作してドキュメントファイルをドキュメント保護プログラム111に受け渡す。ドキュメントファイルを取得したドキュメント保護プログラム111は、ドキュメントファイルにアクセスするために必要となるパスワードと、印刷時に強制したいセキュリティ処理（すなわち、印刷要件）との設定を配布者に要求する。例えば、ドキュメント保護プログラム111は、配布者端末1の表示装置にメッセージを表示するなどして、パスワードと印刷要件の設定を要求する。

【0033】

配布者が配布者端末1の入力装置を介してパスワード及び印刷要件を入力すると、ドキュメント保護プログラム111はこれを取得する。

【0034】

ドキュメント保護プログラム111は、取得したパスワードと印刷要件とを用いてドキュメントファイルから保護ドキュメントを生成する。

【0035】

配布者は、ドキュメント保護プログラム111が生成した保護ドキュメントをユーザに受け渡すとともに、ドキュメントファイルにアクセスするために必要となるパスワードをユーザに通知する。

【0036】

ユーザがドキュメントを印刷しようとする場合には、ユーザ端末102に保護ドキュメントを実装する。例えば、情報記録媒体に記録された保護ドキュメントを外部記録装置を用いてユーザ端末に読み取らせても良いし、ユーザ端末102が配布者端末101と通信可能である場合には、通信網を介して配布者端末101から保護ドキュメントを取得するようにしてもよい。

【0037】

ユーザが、ユーザ端末102の入力装置を介してドキュメント印刷プログラム121に対して印刷を指示すると、印刷を要求されたドキュメント印刷プログラム121は、ドキュメントファイルにアクセスするために必要となるパスワードの入力をユーザに要求する。例えば、ドキュメント印刷プログラム121は、ユーザ端末102の表示装置にメッセージを表示するなどして、パスワードの入力

を要求する。

【0038】

ユーザが、配布者から通知されたパスワードを入力装置を介してユーザ端末102へ入力すると、ドキュメント印刷プログラム121は、入力されたパスワードを用いて保護ドキュメントをドキュメントファイルに復元し、設定されている印刷要件を満たすようにプリンタ103に印刷処理を実行させる。例えば、ドキュメントファイルにBDPが印刷要件として設定されている場合には、ドキュメントの内容とともに地紋画像を印刷する。

【0039】

これにより、ドキュメントファイルを印刷する際に、配布者が設定した印刷要件を強制することが可能となる。

【0040】

ここで、ドキュメント保護プログラム111の動作（保護ドキュメントを生成する処理）及びドキュメント印刷プログラム121の動作（保護ドキュメントを印刷する処理）についてさらに詳しく説明する。

図2に、ドキュメント保護プログラム111の動作を示す。まず、ドキュメント保護プログラム111は、配布者が配布者端末101の入力装置を用いて設定した印刷要件をドキュメントファイルに添付する。

次に、配布者が配布者端末101の入力装置を用いて入力したパスワードを用いて、印刷要件が添付されたドキュメントファイルを暗号化して保護ドキュメントとする。

【0041】

図3に、ドキュメント印刷プログラム121の動作を示す。まず、ドキュメント印刷プログラム121は、ユーザがユーザ端末102の入力装置を用いて入力したパスワードを用いて保護ドキュメントを復号化し、印刷要件が添付されたドキュメントファイルに復元する。次に、ドキュメント印刷プログラム121は、ドキュメントファイルに設定されている印刷要件を満足するようにプリンタドライバを設定し（例えば、印刷要件としてPACが指定されていれば機密印刷モードに設定する）、ドキュメントを印刷する。なお、必要があれば、表示装置にメ

ッセージを表示するなどして、印刷パラメータの設定をユーザに要求するようにしてもよい。

【0042】

ドキュメントファイルに設定されている印刷要件を満足する印刷をプリンタ 103 では実行できない場合、換言すると、プリンタ 103 が設定された印刷要件を満たす機能を備えていない場合には、ドキュメント印刷プログラム 121 は、その旨を示すメッセージをユーザ端末 102 の表示装置に表示させるなどしてユーザに通知し、印刷は行わずに処理を終了する。

【0043】

例えば、印刷要件として P A C が設定されている場合には、ドキュメント印刷プログラム 121 は、印刷を実行する前に P I N の入力进行を要求する。この場合は、印刷実行後、プリンタ 103 のオペレーションパネルにおいて印刷実行前に入力したものと同一の P I N が入力されるまでドキュメントのプリントアウトがプリンタ 103 から出力されない。このため、ドキュメントのプリントアウトがプリンタ 103 に不用意に放置されることがなくなり、プリントアウトによるドキュメントの漏洩を防止することが可能となる。

【0044】

なお、以上の処理においては、保護ドキュメントをパスワードで復号できることを知っている者は、ドキュメント印刷プログラム 121 を介さず、独自にパスワードを用いて保護ドキュメントを復号することも可能ではある。

仮にドキュメント印刷プログラム 121 を介することなく保護ドキュメントを復号した場合には、配布者が設定した印刷要件が強制されることなく、ドキュメントファイルを印刷できてしまう。

【0045】

このため、パスワードのみでドキュメントファイルを暗号化するのではなく、例えば、パスワードとドキュメント保護プログラム 111 の内部に埋め込まれている秘密鍵とを合わせたもの（排他的論理和を取ったものなど）を用いてドキュメントファイルを暗号化するようにしてもよい。

この場合は、ドキュメント印刷プログラム 121 にも同一の秘密鍵を埋め込ん

しておくことで、配布者が設定した印刷要件を印刷時に強制するドキュメント印刷プログラム 121 のみが、保護ドキュメントを復号化して印刷することが可能となる。

【0046】

〔第2の実施形態〕

上記の第1の実施形態においては、ドキュメントファイルをパスワードを用いて保護するドキュメント保護・印刷システムについて説明したが、このシステムでは、パスワードを知っているか否かでドキュメントファイルを印刷できるか否かが決まることとなる。

しかし、実際には、「ユーザAにはドキュメントファイルを印刷させてもよいが、ユーザBには印刷させたくない。さらに、ユーザCがドキュメントファイルを印刷しようとした場合には、プリントアウトに地紋を合成させるようにしたい。」といったように、ユーザ各人に応じて印刷要件を設定したい場合がある。

本発明の第2の実施形態では、このような要求に対応できるドキュメント保護・印刷システムについて説明する。

【0047】

図4に、本実施形態にかかるドキュメント保護・印刷システムの構成を示す。

本実施形態にかかるドキュメント保護・印刷システムは、配布者端末201、ユーザ端末202、プリンタ203及びアクセスコントロールサーバ204を有する。

配布者端末201及びユーザ端末202は、第1の実施形態と同様に、表示装置（例えば、LCD）、入力装置（例えば、キーボード）、外部記録装置（例えば、FDD、HDD）などを備えたコンピュータ端末を適用できる。なお、配布者端末201にはドキュメント保護プログラム211が、ユーザ端末202にはドキュメント印刷プログラム221がそれぞれ実装されている。

【0048】

ドキュメント保護プログラム211は、ドキュメントファイルに配布者端末201の使用者（配布者）の入力操作に応じて処理要件を設定するとともに、暗号化アルゴリズム（RC4、Triple DES、IDEAなど）を用いてドク

ュメントファイルを暗号化し、保護ドキュメントを生成する処理を行うプログラムである。

【0 0 4 9】

ドキュメント印刷プログラム 2 2 1 は、ユーザ端末 2 0 2 の使用者（ユーザ）の入力操作に応じ、保護ドキュメントを復号化するとともに処理要件の一部として設定されている印刷要件に応じた印刷処理をプリンタ 2 0 3 に実行させる処理を行うプログラムである。

【0 0 5 0】

アクセスコントロールサーバ 2 0 4 は、ユーザがドキュメントにアクセス（例えば、印刷）しようとする場合に、ドキュメント印刷プログラム 2 2 1 からの要求に応じて A C L を参照し、ドキュメントにアクセスする権限があるか否か、処理要件がどのように設定されているかを取得するサーバである。

アクセスコントロールサーバ 2 0 4 には、ユーザ各人の認証用の情報（ユーザ名とパスワードとの組）が格納されたユーザデータベース 2 4 1 と、ユーザ各人ごとに設定された処理要件（印刷処理の要件を特に印刷要件という）を含むアクセスコントロールリスト（Access Control List : A C L）が登録される A C L データベース 2 4 2 とが接続されている。

なお、A C L の構造例を図 5 に示す。A C L はユーザ名（User name）、アクセスタイプ（Access type）、許可情報（Permission）及び処理要件（Requirement）をパラメータとして構成される。

【0 0 5 1】

本実施形態にかかるドキュメント保護・印刷システムの動作について説明する。最初にシステム全体の動作について説明する。

配布者は、配布者端末 2 0 1 を操作してこれにドキュメントファイルを実装しておく。例えば、入力装置を用いて配布者がドキュメントファイルを作成してもよいし、外部記録装置を用いて情報記録媒体に記録されたドキュメントファイルを読み取らせても良い。

【0 0 5 2】

ドキュメントファイルにセキュリティを設定する場合、配布者は配布者端末 2

0 1 の入力装置を操作してドキュメントファイルをドキュメント保護プログラム 2 1 1 に受け渡す。ドキュメントファイルを取得したドキュメント保護プログラム 2 1 1 は、A C L の設定を配布者に要求する。例えば、ドキュメント保護プログラム 2 1 1 は、配布者端末 2 0 1 の表示装置にメッセージを表示するなどして、A C L の設定を要求する。

【0 0 5 3】

配布者が配布者端末 2 0 1 の入力装置を介して A C L を設定すると、ドキュメント保護プログラム 2 1 1 はこれを取得する。

【0 0 5 4】

A C L を取得したドキュメント保護プログラム 2 1 1 は、ドキュメントファイルごとに固有のドキュメント I D (Document ID) を生成し、復号に使用する暗号鍵 (Key) と A C L とをこれに関連づけてアクセスコントロールサーバ 2 0 4 へ送信し、A C L データベース 2 4 2 への登録を要求する。

また、ドキュメント保護プログラム 2 1 1 は、暗号鍵を用いて暗号化したドキュメントファイルに対してドキュメント I D を付加して保護ドキュメントを生成する。

【0 0 5 5】

配布者は、ドキュメント保護プログラム 2 1 1 が生成した保護ドキュメントをユーザに受け渡す。

【0 0 5 6】

ユーザがドキュメントを印刷しようとする場合には、ユーザ端末 2 0 2 に保護ドキュメントを実装する。例えば、情報記録媒体に記録された保護ドキュメントを外部記録装置を用いてユーザ端末に読み取らせても良いし、ユーザ端末 2 0 2 が配布者端末 2 0 1 と通信可能である場合には、通信網を介して配布者端末 2 0 1 から保護ドキュメントを取得するようにしてもよい。

【0 0 5 7】

ユーザが、ユーザ端末 2 0 2 の入力装置を介してドキュメント印刷プログラム 2 2 1 に対して印刷を指示すると、印刷を要求されたドキュメント印刷プログラム 2 2 1 は、ユーザを認証するために必要となるユーザ名とパスワードとの入力

をユーザに要求する。例えば、ドキュメント印刷プログラム 2 2 1 は、ユーザ端末 2 0 2 の表示装置にメッセージを表示するなどして、ユーザ名とパスワードとの入力を要求する。

【0 0 5 8】

ドキュメント印刷プログラム 2 2 1 は、ユーザから入力されたユーザ名とパスワードとをアクセスコントロールサーバ 2 0 4 へ送信して、ユーザ認証を要求する。

【0 0 5 9】

アクセスコントロールサーバ 2 0 4 は、ドキュメント印刷プログラム 2 2 1 から受け渡されたユーザ名とパスワードとを用いてユーザ認証を行い、ユーザを特定する。

ユーザを特定すると、アクセスコントロールサーバ 2 0 4 は、ACL データベース 2 4 2 を参照し、ドキュメントファイルを印刷する権限がユーザにあるか否かや、ユーザがドキュメントファイルを印刷する際には、どのような印刷要件が設定されているかを取得する。

ユーザにドキュメントファイルを印刷する権限がある場合、アクセスコントロールサーバ 2 0 4 は、その旨を示す認証情報とともに、保護ドキュメントを復号化するための暗号鍵とユーザがドキュメントファイルを印刷する際の印刷要件とをユーザ端末 2 0 2 を介してドキュメント印刷プログラム 2 2 1 に通知する。

【0 0 6 0】

アクセスコントロールサーバ 2 0 4 から認証情報とともに、暗証鍵と印刷要件とを取得したドキュメント印刷プログラム 2 2 1 は、暗号鍵を用いて保護ドキュメントを復号化してドキュメントファイルに復元する。

そしてドキュメント印刷プログラム 2 2 1 は、印刷要件を満たすようにプリンタ 2 0 3 に印刷処理を実行させる。例えば、ドキュメントファイルに BDP が印刷要件として設定されている場合には、ドキュメントの内容とともに地紋画像を印刷する。

【0 0 6 1】

これにより、ドキュメントファイルを印刷する際に、配布者がユーザ各人に対

して設定した印刷要件を強制することが可能となる。

【0062】

ここで、ドキュメントを保護する際のドキュメント保護プログラム 211 及びアクセスコントロールサーバ 204 の動作、及び保護ドキュメントをドキュメントファイルに復元して印刷する際のドキュメント印刷プログラム 221 及びアクセスコントロールサーバ 204 の動作についてさらに詳しく説明する。

【0063】

図 6 に、ドキュメント保護プログラム 211 が保護ドキュメントを生成する際の動作を示す。ドキュメント保護プログラム 211 は、配布者端末 201 の入力装置における配布者の入力操作によってドキュメントファイルと ACL とを取得すると、ドキュメントファイルの暗号化・復号化するための暗号鍵を生成する。そして、ドキュメント保護プログラム 211 は、生成した暗号鍵を用いてドキュメントファイルを暗号化して、暗号化ドキュメントを生成する。

【0064】

さらにドキュメント保護プログラム 211 は、ドキュメントファイルごとに固有のドキュメント ID を暗号化ドキュメントに添付して保護ドキュメントを生成する。

【0065】

保護ドキュメントを生成した後、ドキュメント保護プログラム 211 は配布者端末 201 の通信機能を用いて、暗号鍵と ACL とドキュメント ID とをアクセスコントロールサーバ 204 へ送信し、これらの登録をアクセスコントロールサーバ 204 に要求する。

【0066】

暗号鍵と ACL とドキュメント ID とをドキュメント保護プログラム 211 から受け渡されたアクセスコントロールサーバ 204 は、図 7 に示すように、これらに関連づけて一つのレコードとして ACL データベース 242 に記録保持する。

【0067】

なお、上記の例においてはドキュメント ID の生成や暗号鍵の生成をドキュメ

ント保護プログラム 2 1 1 が行う場合を示したが、これらの処理はアクセスコントロールサーバ 2 0 4 や不図示のサーバなどで行っても良い。

また、配布者端末 2 0 1 とアクセスコントロールサーバ 2 0 4 との間が専用回線ではなくネットワーク網を介して接続されており、暗号鍵など送信する際に盗聴される懸念がある場合には、SSL (Secure Socket Layer) を用いて通信を行えばよい。

【0 0 6 8】

ドキュメント保護プログラム 2 1 1 がアクセスコントロールサーバ 2 0 4 と通信する際のプロトコルは、どのようなものを用いてもよい。例えば、分散オブジェクト環境を導入し、Java (R) RMI (Remote Method Invocation) や SOAP (Simple Object Access Protocol) をベースとして情報を送受信するようにしても良い。その場合、アクセスコントロールサーバ 2 0 4 は、例えば register(String docId, byte[] key, byte[] acl) のようなメソッドを実装するようにしてもよい。SOAP であれば、HTTPS の上で SOAP プロトコルをやりとりし、RMI であれば SSL ベースの SocketFactory を用いて RMI を実行するようにすれば、ネットワーク上でのセキュリティを確保できる。

【0 0 6 9】

次に、ドキュメント印刷プログラム 2 2 1 が保護ドキュメントを印刷する際の動作について説明する。

図 8 に、保護ドキュメントを印刷する際のドキュメント印刷プログラム 2 2 1 及びアクセスコントロールサーバ 2 0 4 の動作の流れを示す。

ドキュメント印刷プログラム 2 1 は、ユーザ端末 2 の入力装置におけるユーザの入力操作によって保護ドキュメントとユーザ名とパスワードとを取得すると、保護ドキュメントに添付されているドキュメント ID を取得する。

そして、ユーザ名とパスワードとドキュメント ID とアクセスタイプ (ユーザが要求する処理を示す情報。ここでは、保護ドキュメントを印刷しようとするので、“print” となる。) とをアクセスコントロールサーバ 2 0 4 へ送信して、アクセス権限があるか否かのチェックを要求する。

【0 0 7 0】

アクセスコントロールサーバ204は、ドキュメント印刷プログラム221からユーザ名とパスワードとドキュメントIDとアクセスタイプとを取得すると、ユーザデータベース241に登録されている情報を参照し、ユーザ認証を行う。

換言すると、アクセスコントロールサーバ204は、ユーザデータベース241に登録されている情報を参照し、ドキュメント印刷プログラム221から取得した情報に含まれるユーザ名とパスワードとを組としたものが、ユーザデータベース241に組として登録されているか否かを判断する。

【0071】

ユーザ認証に失敗した場合（換言すると、ドキュメント印刷プログラム221から受け渡された情報に含まれるユーザ名とパスワードとを組としたものがユーザデータベース241に登録されていない場合）、アクセスコントロールサーバ204は、許可情報（ユーザが要求する処理を許可するか否かを示す情報）を「不許可」としてユーザ端末202へ送信し、ドキュメント印刷プログラム221へ受け渡す。なお、この場合は「エラー」とした許可情報をドキュメント印刷プログラム221へ受け渡すようにしてもよい。

【0072】

一方、ユーザ認証に成功した場合、アクセスコントロールサーバ204は、ACLデータベース242に格納されているレコードのうち、ドキュメント印刷プログラム221から取得した情報に含まれるドキュメントIDに関するレコードを読み出す。

【0073】

アクセスコントロールサーバ204は、読み出したレコードに含まれるACLを取得し、ドキュメント印刷プログラム221から取得したユーザ名及びアクセスタイプに基づいて、ACLから許可情報および印刷要件を取得する。

換言すると、アクセスコントロールサーバ204は、ユーザ名とアクセスタイプとに基づいて、予めACLに設定されている許可情報と印刷要件とを取得する。

【0074】

ACLから取得した許可情報が「許可」である場合、アクセスコントロールサ

サーバ 2 0 4 は、レコードに格納されている暗号鍵と印刷要件とを許可情報とともにユーザ端末 2 0 2 へ送信してドキュメント印刷プログラム 2 2 1 に受け渡す。

一方、ACL から取得した許可情報が「不許可」である場合、アクセスコントロールサーバ 2 0 4 は、許可情報のみをユーザ端末 2 0 2 へ送信してドキュメント印刷プログラム 2 2 1 に受け渡す。

【0 0 7 5】

アクセスコントロールサーバ 2 0 4 から許可情報を受け渡されたドキュメント印刷プログラム 2 2 1 は、取得した許可情報を参照し、「不許可」である場合には、ユーザ端末 2 0 2 の表示装置にメッセージを表示するなどして、要求された処理を実行できないことをユーザに通知する。

【0 0 7 6】

一方、取得した許可情報が「許可」である場合には、許可情報と共に受け渡された暗号鍵を用いて、保護ドキュメントのうちの暗号化ドキュメントの部分を復号化してドキュメントファイルに復元する。

また、ドキュメント印刷プログラム 2 2 1 は、許可情報と共に取得した印刷要件を満たすようにプリンタドライバを設定し（例えば、PAC が指定されていれば機密印刷モードに設定する）、プリンタ 2 0 3 にドキュメントの印刷処理を実行させる。

なお、必要があれば、ユーザ端末 2 0 2 の表示装置にメッセージを表示するなどして、印刷パラメータの設定をユーザに要求するようにしてもよい。

【0 0 7 7】

アクセスコントロールサーバ 2 0 4 から取得した印刷要件を満たす印刷をプリンタ 2 0 3 では実行できない場合、換言すると、プリンタ 2 0 3 が ACL に設定されていた印刷要件を満たす機能を備えていない場合には、その旨を示すメッセージを表示装置に表示させるなどしてユーザに通知し、印刷は行わずに処理を終了する。

【0 0 7 8】

以上の動作によって、ユーザごとに異なるアクセス権や印刷要件を設定することが可能となる。また、上記のように、サーバ側でドキュメントファイルに対す

るアクセス権限を判断するシステム構成においては、ACLデータベース 2 4 2 に登録されている ACL の内容を配布者端末 2 0 1 やアクセスコントロールサーバ 2 0 4 における入力操作によって変更できるようにしてもよく、この場合には、保護ドキュメントを配布した後で印刷要件を変更したりすることが可能となる。

例えば、既に配布した保護ドキュメントに対するアクセス権限を新たなユーザに設定したり、特定のユーザに対して印刷要件を追加することなどが可能となる。

【0 0 7 9】

なお、本実施形態にかかるドキュメント保護・印刷システムが上記のような手法でドキュメントファイルを保護していることを知っている者は、ドキュメント印刷プログラム 2 2 1 に成りすますプログラムをコンピュータ端末に実行させて暗号鍵を不正に入手し、保護ドキュメントを復号化することも可能ではある。この場合は、ACL として設定されている印刷要件を強制されることなく、保護ドキュメントを印刷できてしまうこととなる。

【0 0 8 0】

このため、単に暗号鍵のみを用いてドキュメントファイルを暗号化するのではなく、ドキュメント保護プログラム 2 1 1 の内部に埋め込まれた秘密鍵と暗号鍵とを合わせたもの（排他的論理和を取ったもの）でドキュメントファイルを暗号化することが好ましい。

この場合は、ドキュメント印刷プログラム 2 2 1 にも同一の秘密鍵を埋め込んでおくことで、配布者が設定した印刷要件を印刷時に強制するドキュメント印刷プログラム 2 2 1 のみが、保護ドキュメントを復号化して印刷することが可能となる。

【0 0 8 1】

また、本実施形態においては、ドキュメント印刷プログラム 2 2 1 は、ドキュメントファイルの印刷に関する処理のみを行っているが、ドキュメント印刷プログラム 2 2 1 は、ドキュメントファイルの内容をユーザに提示したり、ドキュメントファイルを編集する機能を備えていても良い。例えば、Adobe Acrobat の pl

ug-in としてこの機能を実現することが可能である。

【0082】

〔第3の実施形態〕

本発明を好適に実施した第3の実施形態について説明する。

上記本発明の第2の実施形態においては、配布者がドキュメントファイルに対してACLを設定する必要がある。このため、多数のユーザにドキュメントを配布しようとする場合は、各ユーザごとに印刷要件を個別に設定することはドキュメントファイルの配布者がACLを作成するための負担が大きくなってしまう。

【0083】

一方、ドキュメントファイルの内容がビジネス文書などである場合は、これをどのように保護するかは、配布者が独自に決定するのではなく、所属する組織（企業や団体など）のセキュリティポリシー（秘密管理規則）に基づいて決定することとなる。よって、ドキュメント保護・印刷システムが配布者の所属する組織のセキュリティーポリシーに従ってドキュメントファイルを保護できれば、配布者がACLを設定しなくても良くなる。

本発明の第3の実施形態では、配布者の所属する組織のセキュリティーポリシーに従ってドキュメントを保護するドキュメント保護・印刷システムについて説明する。

【0084】

図9に、本実施形態にかかるドキュメント保護・印刷システムの構成を示す。

本実施形態にかかるドキュメント保護・印刷システムは、配布者端末301、ユーザ端末302、プリンタ303及びアクセスコントロールサーバ304を有する。

配布者端末301及びユーザ端末302は、第1の実施形態と同様に、表示装置（例えば、LCD）、入力装置（例えば、キーボード）、外部記録装置（例えば、FDD、HDD）などを備えたコンピュータ端末を適用できる。なお、配布者端末301にはドキュメント保護プログラム311が、ユーザ端末302にはドキュメント印刷プログラム321がそれぞれ実装されている。

【0085】

ドキュメント保護プログラム 3 1 1 は、ドキュメントファイルに配布者端末 3 0 1 の使用者（配布者）の入力操作に応じて処理要件を設定するとともに、暗号化アルゴリズム（RC4、Triple DES、IDEA など）を用いてドキュメントファイルを暗号化し、保護ドキュメントを生成する処理を行うプログラムである。

【0 0 8 6】

ドキュメント印刷プログラム 3 2 1 は、ユーザ端末 3 0 2 の使用者（ユーザ）の入力操作に応じ、保護ドキュメントを復号化するとともに設定されている印刷要件に応じた印刷処理をプリンタ 3 0 3 に実行させる処理を行うプログラムである。

【0 0 8 7】

アクセスコントロールサーバ 3 0 4 は、ユーザがドキュメントにアクセス（例えば、印刷）しようとする場合に、ドキュメント印刷プログラム 3 2 1 からの要求に応じて ACL を参照し、ドキュメントにアクセスする権限があるか否か、処理要件がどのように設定されているかを取得するサーバである。

アクセスコントロールサーバ 3 0 4 には、ユーザ各人の認証用の情報（ユーザ名とパスワードとの組）及びユーザの階級を示す情報が格納されたユーザデータベース 3 4 1 と、ユーザ各人ごとに設定された処理要件を含むアクセスコントロールリスト（Access Control List : ACL）がセキュリティ属性に応じて複数登録されている ACL データベース 3 4 2 と、各保護ドキュメントにどのようなセキュリティ属性が設定されているかを示す情報及びその保護ドキュメントを復号化するための暗証鍵が関連づけられて登録されるセキュリティ属性データベース 3 4 3 とが接続されている。なお、セキュリティ属性に応じた ACL の一例をあげると、「第一設計室用 ACL」、「第二設計室用 ACL」のように小組織に応じた ACL である。

【0 0 8 8】

本実施形態にかかるドキュメント保護・印刷システムの動作について説明する。最初にシステム全体の動作について説明する。

配布者は、配布者端末 3 0 1 を操作してこれにドキュメントファイルを実装し

ておく。例えば、入力装置を用いて配布者がドキュメントファイルを作成してもよいし、外部記録装置を用いて情報記録媒体に記録されたドキュメントファイルを読み取らせても良い。

【0089】

ドキュメントファイルにセキュリティを設定する場合、配布者は配布者端末 301 の入力装置を操作してドキュメントファイルをドキュメント保護プログラム 311 に受け渡す。ドキュメントファイルを取得したドキュメント保護プログラム 311 は、セキュリティ属性の設定を配布者に要求する。例えば、ドキュメント保護プログラム 311 は、配布者端末 1 の表示装置にメッセージを表示するなどして、セキュリティ属性の設定を要求する。

【0090】

配布者が配布者端末 301 の入力装置を介してドキュメントファイルにセキュリティ属性を設定すると、ドキュメント保護プログラム 311 はこれを取得する。

【0091】

セキュリティ属性を取得したドキュメント保護プログラム 311 は、ドキュメントファイルごとに固有のドキュメント ID を生成し、復号に使用する暗号鍵とセキュリティ属性とをこれに関連づけてアクセスコントロールサーバ 304 へ送信し、セキュリティ属性データベース 343 への登録を要求する。

また、ドキュメント保護プログラム 311 は、暗号鍵を用いて暗号化したドキュメントファイルに対してドキュメント ID を付加して保護ドキュメントを生成する。

【0092】

配布者は、ドキュメント保護プログラム 311 が生成した保護ドキュメントをユーザに受け渡す。

【0093】

ユーザがドキュメントを印刷しようとする場合には、ユーザ端末 302 に保護ドキュメントを実装する。例えば、情報記録媒体に記録された保護ドキュメントを外部記録装置を用いてユーザ端末に読み取らせても良いし、ユーザ端末 302

が配布者端末 3 0 1 と通信可能である場合には、通信網を介して配布者端末 3 0 1 から保護ドキュメントを取得するようにしてもよい。

【0 0 9 4】

ユーザが、ユーザ端末 3 0 2 の入力装置を介してドキュメント印刷プログラム 3 2 1 に対して印刷を指示すると、印刷を要求されたドキュメント印刷プログラム 3 2 1 は、ユーザを認証するために必要となるユーザ名とパスワードとの入力をユーザに要求する。例えば、ドキュメント印刷プログラム 3 2 1 は、ユーザ端末 3 0 2 の表示装置にメッセージを表示するなどして、ユーザ名とパスワードとの入力を要求する。

【0 0 9 5】

ドキュメント印刷プログラム 3 2 1 は、ユーザから入力されたユーザ名とパスワードとをアクセスコントロールサーバ 3 0 4 へ送信して、ユーザ認証を要求する。

【0 0 9 6】

アクセスコントロールサーバ 3 0 4 は、ドキュメント印刷プログラム 3 2 1 から受け渡されたユーザ名とパスワードとを用いてユーザ認証を行い、ユーザを特定する。

【0 0 9 7】

ユーザを特定すると、アクセスコントロールサーバ 3 0 4 は、セキュリティ属性データベース 3 4 3 を参照し、保護ドキュメントに設定されているセキュリティ属性の種類を特定する。その後、アクセスコントロールサーバ 3 0 4 は、ACL データベース 3 4 2 に登録されている ACL のうち、保護ドキュメントに設定されているセキュリティ属性に該当するものを参照し、ドキュメントファイルを印刷する権限がユーザにあるか否かや、ユーザがドキュメントファイルを印刷する際には、どのような印刷要件が設定されているかを取得する。

【0 0 9 8】

ユーザにドキュメントファイルを印刷する権限がある場合、アクセスコントロールサーバ 3 0 4 は、印刷が許可されていることを示す許可情報とともに、保護ドキュメントを復号化するための暗号鍵とユーザがドキュメントファイルを印刷

する際の印刷要件とをユーザ端末 3 0 2 へ送信し、ドキュメント印刷プログラム 3 2 1 に受け渡す。

【0 0 9 9】

アクセスコントロールサーバ 3 0 4 から許可情報とともに、暗証鍵と印刷要件とを取得したドキュメント印刷プログラム 3 2 1 は、暗号鍵を用いて保護ドキュメントを復号化してドキュメントファイルに復元する。

そしてドキュメント印刷プログラム 3 2 1 は、印刷要件を満たすようにプリンタ 3 0 3 に印刷処理を実行させる。例えば、ドキュメントファイルに B D P が印刷要件として設定されている場合には、ドキュメントの内容とともに地紋画像を印刷する。

【0 1 0 0】

これにより、ドキュメントファイルを印刷する際に、予め設定されたセキュリティ属性に応じた印刷要件を強制することが可能となる。

【0 1 0 1】

ここで、ドキュメントを保護する際のドキュメント保護プログラム 3 1 1 及びアクセスコントロールサーバ 3 0 4 の動作、及び保護ドキュメントをドキュメントファイルに復元して印刷する際のドキュメント印刷プログラム 3 2 1 及びアクセスコントロールサーバ 3 0 4 の動作についてさらに詳しく説明する。

【0 1 0 2】

図 1 0 に、ドキュメント保護プログラム 3 1 1 が保護ドキュメントを生成する際の動作を示す。ドキュメント保護プログラム 3 1 1 は、配布者端末 3 0 1 の入力装置における配布者の入力操作によってドキュメントファイルとそのセキュリティ属性とを取得すると、ドキュメントファイルを暗号化・復号化するための暗号鍵を生成する。そして、ドキュメント保護プログラム 3 1 1 は、生成した暗号鍵を用いてドキュメントファイルを暗号化し、暗号化ドキュメントを生成する。

【0 1 0 3】

さらにドキュメント保護プログラム 3 1 1 は、ドキュメントファイルごとに固有のドキュメント I D を暗号化ドキュメントに添付して保護ドキュメントを生成する。

【 0 1 0 4 】

保護ドキュメントを生成した後、ドキュメント保護プログラム 3 1 1 は配布者端末 3 0 1 の通信機能を用いて、暗号鍵とセキュリティ属性とドキュメント I D とをアクセスコントロールサーバ 3 0 4 へ送信し、これらの登録をアクセスコントロールサーバ 3 0 4 に要求する。

【 0 1 0 5 】

暗号鍵とセキュリティ属性とドキュメント I D とをドキュメント保護プログラム 3 1 1 から受け渡されたアクセスコントロールサーバ 3 0 4 は、これらに関連づけて一つのレコードとしてセキュリティ属性データベース 3 4 3 に登録し、記録保持する。

【 0 1 0 6 】

なお、上記の例においてはドキュメント I D の生成や暗号鍵の生成をドキュメント保護プログラム 3 1 1 が行う場合を示したが、これらの処理はアクセスコントロールサーバ 3 0 4 や不図示のサーバなどで行っても良い。

また、配布者端末 3 0 1 とアクセスコントロールサーバ 3 0 4 との間が専用回線ではなくネットワーク網を介して接続されており、暗号鍵など送信する際に盗聴される懸念がある場合には、S S L (Secure Socket Layer) を用いて通信を行えばよい。

【 0 1 0 7 】

ドキュメント保護プログラム 3 1 1 がアクセスコントロールサーバ 3 0 4 と通信する際のプロトコルは、どのようなものを用いてもよい。例えば、分散オブジェクト環境を導入し、J a v a (R) R M I (Remote Method Invocation) や S O A P (Simple Object Access Protocol) をベースとして情報を送受信するようにしてもよい。その場合、アクセスコントロールサーバ 3 0 4 は、例えばregister(String docId,byte[] key,byte[] acl)のようなメソッドを実装するようにしてもよい。S O A Pであれば、H T T P Sの上でS O A Pプロトコルをやりとりし、R M IであればS S LベースのSocketFactoryを用いてR M Iを実行するようにすれば、ネットワーク上でのセキュリティを確保することができる。

【 0 1 0 8 】

次に、ドキュメント印刷プログラム 321 が保護ドキュメントを印刷する際の動作について説明する。

図 11 に、ドキュメント印刷プログラム 321 が行う処理の内容を示す。また、図 12 に、ドキュメント印刷プログラム 321 及びアクセスコントロールサーバ 304 の動作の流れを示す。

ドキュメント印刷プログラム 321 は、ユーザ端末 302 の入力装置におけるユーザの入力操作によって保護ドキュメントとユーザ名とパスワードとを取得すると、保護ドキュメントに添付されているドキュメント ID を取得する。

そして、ユーザ名とパスワードとドキュメント ID とアクセスタイプ（ユーザが要求する処理を示す情報。ここでは、保護ドキュメントを印刷しようとするので、“print” となる。）とをアクセスコントロールサーバ 304 へ送信して、アクセス権限があるか否かのチェックを要求する。

【0109】

アクセスコントロールサーバ 304 は、ドキュメント印刷プログラム 321 からユーザ名とパスワードとドキュメント ID とアクセスタイプとを取得すると、ユーザデータベース 341 に登録されている情報を参照し、ユーザ認証を行う。

換言すると、アクセスコントロールサーバ 304 は、ユーザデータベース 341 に登録されている情報を参照し、ドキュメント印刷プログラム 321 から取得した情報に含まれるユーザ名とパスワードとの組と一致するものが、ユーザデータベース 341 に登録されているか否かを判断する。

【0110】

ユーザ認証に失敗した場合（換言すると、ドキュメント印刷プログラム 321 から受け渡された情報に含まれるユーザ名とパスワードとを組としたものがユーザデータベース 341 に登録されていない場合）、アクセスコントロールサーバ 304 は、許可情報（ユーザが要求する処理を許可するか否かを示す情報）を「不許可」としてユーザ端末 302 へ送信し、ドキュメント印刷プログラム 321 へ受け渡す。なお、この場合は「エラー」とした許可情報をドキュメント印刷プログラム 321 へ受け渡すようにしてもよい。

【0111】

一方、ユーザ認証に成功した場合、アクセスコントロールサーバ4は、セキュリティ属性データベース343に登録されているレコードのうち、ドキュメント印刷プログラム321から取得した情報に含まれるドキュメントIDに関するレコードを読み出す。

【0112】

アクセスコントロールサーバ304は、読み出したレコードに含まれるセキュリティ属性を取得する。そして、アクセスコントロールサーバ304は、ACLデータベース342に登録されているACLのうち、レコードから取得したセキュリティ属性に応じたACLを読み出して取得する。さらに、アクセスコントロールサーバ304は、ドキュメント印刷プログラム321から取得したユーザ名及びアクセスタイプに基づいて、ACLから許可情報および印刷要件を取得する。

換言すると、アクセスコントロールサーバ304は、ユーザ名とアクセスタイプとに基づいて、予めACLに設定されている許可情報と印刷要件とを取得する。

【0113】

ACLから取得した許可情報が「許可」である場合、アクセスコントロールサーバ304は、レコードに格納されている暗号鍵と印刷要件とを許可情報とともにユーザ端末302へ送信してドキュメント印刷プログラム321に受け渡す。

一方、ACLから取得した許可情報が「不許可」である場合、アクセスコントロールサーバ304は、許可情報のみをユーザ端末302へ送信してドキュメント印刷プログラムに受け渡す。

【0114】

アクセスコントロールサーバ304から許可情報を受け渡されたドキュメント印刷プログラム321は、取得した許可情報を参照し、「不許可」である場合には、表示装置にメッセージを表示するなどして、要求された処理を実行できないことをユーザに通知する。

【0115】

一方、取得した許可情報が「許可」である場合には、許可情報と共に受け渡さ

れた暗号鍵を用いて、保護ドキュメントのうちの暗号化ドキュメントの部分を復号化してドキュメントファイルに復元する。

また、ドキュメント印刷プログラム 3 2 1 は、許可情報と共に取得した印刷要件を満足するようにプリンタドライバを設定し（例えば、P A C が指定されていれば機密印刷モードに設定する）、プリンタ 3 0 3 にドキュメントの印刷処理を実行させる。

なお、必要があれば、表示装置にメッセージを表示するなどして、印刷パラメータの設定をユーザに要求するようにしてもよい。

【 0 1 1 6 】

アクセスコントロールサーバ 3 0 4 から取得した印刷要件を満足する印刷をプリンタ 3 0 3 では実行できない場合、換言すると、プリンタ 3 0 3 が A C L に設定されていた印刷要件を満たす機能を備えていない場合には、ドキュメント印刷プログラム 3 2 1 は、その旨を示すメッセージを表示装置に表示させるなどしてユーザに通知し、印刷は行わずに処理を終了する。

【 0 1 1 7 】

以上の動作によって、ユーザごとに異なるアクセス権や印刷要件を設定することが可能となる。また、上記のように、サーバ側でドキュメントファイルに対するアクセス権限を判断するシステム構成においては、A C L データベース 3 4 2 に登録されている A C L の内容を配布者端末 3 0 1 やアクセスコントロールサーバ 3 0 4 における入力操作によって変更できるようにしてもよく、この場合には、保護ドキュメントを配布した後で印刷要件を変更したりすることが可能となる。

例えば、既に配布した保護ドキュメントに対するアクセス権限を新たなユーザに設定したり、特定のユーザに対して印刷要件を追加することなどが可能となる。

【 0 1 1 8 】

なお、本実施形態にかかるドキュメント保護・印刷システムが上記のような手法でドキュメントファイルを保護していることを知っている者は、ドキュメント印刷プログラム 3 2 1 に成りすますプログラムをコンピュータ端末に実行させて

暗号鍵を不正に入手し、保護ドキュメントを復号化することも可能ではある。この場合は、ACLとして設定されている印刷要件を強制されることなく、保護ドキュメントを印刷できてしまうこととなる。

【0 1 1 9】

このため、単に暗号鍵のみを用いてドキュメントファイルを暗号化するのではなく、ドキュメント保護プログラム 3 1 1 の内部に埋め込まれた秘密鍵と暗号鍵とを合わせたもの（排他的論理和を取ったもの）でドキュメントファイルを暗号化することが好ましい。

この場合は、ドキュメント印刷プログラム 3 2 1 にも同一の秘密鍵を埋め込んでおくことで、配布者が設定した印刷要件を印刷時に強制するドキュメント印刷プログラム 3 2 1 のみが、保護ドキュメントを復号化して印刷することが可能となる。

【0 1 2 0】

なお、本実施形態においては、ドキュメント印刷プログラム 3 2 1 は、ドキュメントファイルの印刷に関する処理のみを行っているが、ドキュメント印刷プログラム 3 2 1 は、ドキュメントファイルの内容をユーザに提示したり、ドキュメントファイルを編集する機能を備えていても良い。例えば、Adobe Acrobat の plug-in としてこの機能を実現することが可能である。

【0 1 2 1】

このように、本実施形態にかかるドキュメント保護・印刷システムによれば、セキュリティ属性に応じて予めACLとして設定されている印刷要件を、ドキュメントファイルを印刷する際に強制することが可能となる。

【0 1 2 2】

〔第 4 の実施形態〕

上記本発明の第 3 の実施形態においては、配布者の所属する組織のセキュリティポリシーに従ってドキュメントを保護するドキュメント保護・印刷システムについて説明した。

しかし、第 3 の実施形態にかかるドキュメント保護・印刷システムは、配布者が所属する組織の規模が大きい場合は、その下位組織ごとに数多くのACLを予

め定義して登録しておかなければならない。例えば、「第一設計室の技術文書用 A C L」、「第一設計室の契約書用 A C L」、「第二設計室の技術文書用 A C L」、「第二設計室の契約書用 A C L」のように、各ユーザを網羅するように A C L を予め定義しておく必要がある。

【 0 1 2 3 】

一般に、組織の掲げるセキュリティポリシーは総則的なものであり、誰にどのドキュメントファイルに対するアクセスを許可するかといったことまでを規定するものではない。

組織の掲げるセキュリティポリシーの一例を図 1 3 に示す。図に示すように、組織におけるセキュリティポリシーは、ドキュメントに対して機密レベル（Sensitivity）及び分野（Category）を設定した上で、ドキュメントに対するアクセスを許可するユーザの階級（Level）や部門（Category）及びその印刷要件を設定したものであるといえる。

例えば、機密レベルが極秘（Top Secret）の人事関連（Human Resource）のドキュメントは、人事部の管理職のみが地紋印刷を条件として印刷可能という具合である。

本発明の第 4 の実施形態では、組織の掲げるセキュリティーポリシーをそのままの形で電子的に記述したものをドキュメントファイルの保護に適用したドキュメント保護・印刷システムについて説明する。

【 0 1 2 4 】

図 1 4 に、本実施形態にかかるドキュメント保護・印刷システムの構成を示す。

本実施形態にかかるドキュメント保護・印刷システムは、配布者端末 4 0 1、ユーザ端末 4 0 2、プリンタ 4 0 3 及びアクセスコントロールサーバ 4 0 4 を有する。

配布者端末 4 0 1 及びユーザ端末 4 0 2 は、第 1 の実施形態と同様に、表示装置（例えば、L C D）、入力装置（例えば、キーボード）、外部記録装置（例えば、F D D、H D D）などを備えたコンピュータ端末を適用できる。なお、配布者端末 4 0 1 にはドキュメント保護プログラム 4 1 1 が、ユーザ端末 4 0 2 には

ドキュメント印刷プログラム 4 2 1 がそれぞれ実装されている。

【0 1 2 5】

ドキュメント保護プログラム 4 1 1 は、ドキュメントファイルに配布者端末 4 0 1 の使用者（配布者）の入力操作に応じた処理要件を設定するとともに、暗号化アルゴリズム（RC 4、T r i p l e D E S、I D E A など）を用いてドキュメントファイルを暗号化し、保護ドキュメントを生成する処理を行うプログラムである。

【0 1 2 6】

ドキュメント印刷プログラム 4 2 1 は、ユーザ端末 4 0 2 の使用者（ユーザ）の入力操作に応じ、保護ドキュメントを復号化するとともに設定されている印刷要件に応じた印刷処理をプリンタ 4 0 3 に実行させる処理を行うプログラムである。

【0 1 2 7】

アクセスコントロールサーバ 4 0 4 は、ユーザがドキュメントを印刷しようとする場合に、ドキュメント印刷プログラム 4 2 1 からの要求に応じて自身が記録保持しているセキュリティポリシーを参照し、ドキュメントを印刷する権限があるか否か、印刷要件がどのように設定されているかを取得するサーバである。

【0 1 2 8】

図 1 5 に、アクセスコントロールサーバ 4 0 4 に登録されるセキュリティポリシーの一例を示す。

例えば、カテゴリが「技術文書」で機密レベルが「マル秘」のドキュメントファイルは、カテゴリが「技術」で階級が「中」又は「上」のユーザに対して、閲覧は許可するが R A D を要件とすること、印刷を許可するが P A C と B D P と E B C と R A D とを要件とすること、及び、ハードコピーは許可しないことが規定されている。

アクセスコントロールサーバ 4 0 4 は、セキュリティポリシーのデータをどのような形で記録保持していても構わない。なお、XML (eXtensible Markup Language) を用いれば、図 1 6 に示すように、簡単に記述できる。

【0 1 2 9】

アクセスコントロールサーバ 4 0 4 には、ユーザ各人の認証用の情報（ユーザ名とパスワードとの組）が格納されたユーザデータベース 4 4 1 と、各保護ドキュメントにどのようなセキュリティ属性が設定されているかを示す情報及びその保護ドキュメントを復号化する為の暗証鍵が関連づけられて登録されるセキュリティ属性データベース 4 4 3 とが接続されている。

【0 1 3 0】

図 1 7 に、ユーザデータベース 4 4 1 に登録される情報の一例を示す。

図 1 7 においてはユーザごとにカテゴリと階級とを別々の属性として管理する構造としているが、たとえば、Windows (R) Domain のユーザ管理機構を利用してユーザを管理するような場合には、グループアカウントとして Technical_Medium のようなものを生成し、Ichiro というユーザをそのグループに所属させるようにしてもよい。所属グループの命名規則をこのように設定しておくことで、カテゴリと階級とを管理することが可能となる。

【0 1 3 1】

本実施形態にかかるドキュメント保護・印刷システムの動作について説明する。最初に、システム全体の動作について説明する。

配布者は、配布者端末 4 0 1 を操作してこれにドキュメントファイルを実装しておく。例えば、入力装置を用いて配布者がドキュメントファイルを作成してもよいし、外部記録装置を用いて情報記録媒体に記録されたドキュメントファイルを読み取らせても良い。

【0 1 3 2】

ドキュメントファイルにセキュリティを設定する場合、配布者は配布者端末 4 0 1 の入力装置を操作してドキュメントファイルをドキュメント保護プログラム 4 1 1 に受け渡す。ドキュメントファイルを取得したドキュメント保護プログラム 4 1 1 は、セキュリティ属性の設定を配布者に要求する。例えば、ドキュメント保護プログラム 4 1 1 は、配布者端末 4 0 1 の表示装置にメッセージを表示するなどして、セキュリティ属性の設定を要求する。なお、ここでのセキュリティ属性とは、保護しようとするドキュメントがセキュリティ属性 DB 4 4 3 に登録されているセキュリティ属性のうちのいずれに該当するかを示す情報である。

【0 1 3 3】

配布者が配布者端末 4 0 1 の入力装置を介してドキュメントファイルにセキュリティ属性を設定すると、ドキュメント保護プログラム 4 1 1 はこれを取得する。

【0 1 3 4】

セキュリティ属性を取得したドキュメント保護プログラム 4 1 1 は、ドキュメントファイルごとに固有のドキュメント ID を生成し、復号に使用する暗号鍵とセキュリティ属性とをこれに関連づけてアクセスコントロールサーバ 4 0 4 へ送信し、登録する。

また、ドキュメント保護プログラム 4 1 1 は、暗号鍵を用いて暗号化したドキュメントファイルに対してドキュメント ID を付加して保護ドキュメントを生成する。

【0 1 3 5】

配布者は、ドキュメント保護プログラム 4 1 1 が生成した保護ドキュメントをユーザに受け渡す。

【0 1 3 6】

ユーザがドキュメントを印刷しようとする場合には、ユーザ端末 4 0 2 に保護ドキュメントを実装する。例えば、情報記録媒体に記録された保護ドキュメントを外部記録装置を用いてユーザ端末に読み取らせても良いし、ユーザ端末 4 0 2 が配布者端末 4 0 1 と通信可能である場合には、通信網を介して配布者端末 4 0 1 から保護ドキュメントを取得するようにしてもよい。

【0 1 3 7】

ユーザが、ユーザ端末 4 0 2 の入力装置を介してドキュメント印刷プログラム 4 2 1 に対して印刷を指示すると、印刷を要求されたドキュメント印刷プログラム 4 2 1 は、ユーザを認証するために必要となるユーザ名とパスワードの入力をユーザに要求する。例えば、ドキュメント印刷プログラム 4 2 1 は、ユーザ端末 4 0 2 の表示装置にメッセージを表示するなどして、ユーザ名とパスワードの入力を要求する。

【0 1 3 8】

ドキュメント印刷プログラム 4 2 1 は、ユーザから入力されたユーザ名とパスワードとをアクセスコントロールサーバ 4 へ送信して、ユーザ認証を要求する。

【 0 1 3 9 】

アクセスコントロールサーバ 4 0 4 は、ドキュメント印刷プログラム 4 2 1 から受け渡されたユーザ名とパスワードとを用いてユーザ認証を行い、ユーザを特定する。

【 0 1 4 0 】

ユーザを特定すると、アクセスコントロールサーバ 4 0 4 は、セキュリティ属性データベース 4 4 3 を参照し、保護ドキュメントに設定されているセキュリティ属性の種類を特定する。

アクセスコントロールサーバ 4 0 4 は、ユーザデータベース 4 4 1 から取得したユーザの階級を示す情報及び、ドキュメントに設定されているセキュリティ属性とに基づいて、ドキュメントを印刷する権限がユーザにあるか否かや、ユーザがドキュメントファイルを印刷する際にはどのような印刷要件が設定されているのかを取得する。

【 0 1 4 1 】

ユーザにドキュメントファイルを印刷する権限がある場合、アクセスコントロールサーバ 4 0 4 は、印刷が許可されていることを示す許可情報とともに、保護ドキュメントを復号化するための暗号鍵とユーザがドキュメントファイルを印刷する際の印刷要件とをユーザ端末 4 0 2 へ送信し、ドキュメント印刷プログラム 4 2 1 に受け渡す。

【 0 1 4 2 】

アクセスコントロールサーバ 4 0 4 から許可情報とともに、暗証鍵と印刷要件とを取得したドキュメント印刷プログラム 4 2 1 は、暗号鍵を用いて保護ドキュメントを復号化してドキュメントファイルに復元する。

そしてドキュメント印刷プログラム 4 2 1 は、印刷要件を満たすようにプリンタ 4 0 3 に印刷処理を実行させる。例えば、ドキュメントファイルに B D P が印刷要件として設定されている場合には、ドキュメントの内容とともに地紋画像を印刷する。

【0 1 4 3】

これにより、ドキュメントファイルを印刷する際に、予め設定されたセキュリティ属性に応じた印刷要件を強制することが可能となる。

【0 1 4 4】

ここで、ドキュメントを保護する際のドキュメント保護プログラム 4 1 1 及びアクセスコントロールサーバ 4 0 4 の動作、及び保護ドキュメントをドキュメントファイルに復元して印刷する際のドキュメント印刷プログラム 4 2 1 及びアクセスコントロールサーバ 4 0 4 の動作についてさらに詳しく説明する。

【0 1 4 5】

図 1 8 に、ドキュメント保護プログラム 4 1 1 が保護ドキュメントを生成する際の処理を示す。また、図 1 9 に、ドキュメント保護プログラム 4 1 1 及びアクセスコントロールサーバ 4 0 4 の動作の流れを示す。

ドキュメント保護プログラム 4 1 1 は、配布者端末 4 0 1 の入力装置における配布者の入力操作によってドキュメントファイルとそのセキュリティ属性とを取得すると、ドキュメントファイルを暗号化・復号化するための暗号鍵を生成する。そして、ドキュメント保護プログラム 4 1 1 は、生成した暗号鍵を用いてドキュメントファイルを暗号化して、暗号化ドキュメントを生成する。

【0 1 4 6】

さらに、ドキュメント保護プログラム 4 1 1 は、ドキュメントファイルごとに固有のドキュメント ID を暗号化ドキュメントに添付して保護ドキュメントを生成する。

【0 1 4 7】

保護ドキュメントを生成した後、ドキュメント保護プログラム 4 1 1 は、配布者端末 4 0 1 の通信機能を用いて、暗号鍵とセキュリティ属性とドキュメント ID とをアクセスコントロールサーバ 4 0 4 へ送信し、これらの登録をアクセスコントロールサーバ 4 0 4 に要求する。

【0 1 4 8】

暗号鍵とセキュリティ属性とドキュメント ID とをドキュメント保護プログラム 4 1 1 から受け渡されたアクセスコントロールサーバ 4 0 4 は、これらを一つ

のレコードとしてセキュリティ属性データベース 4 4 3 に記録保持する。

【0 1 4 9】

ここではドキュメント保護プログラム 4 1 1 がドキュメント ID を生成して暗号化ドキュメントに添付する場合を例に挙げたが、SHA-1 のなどのハッシュアルゴリズムを用いて暗号化ドキュメントファイルを生成した場合には、そのハッシュ値をドキュメント ID の代わりに用いてもよい。この場合は、保護ドキュメントにドキュメント ID を添付する必要はなく、後でドキュメント ID を取得したい時は、再度ハッシュ値を計算すれば良い。

【0 1 5 0】

なお、上記の例においてはドキュメント ID の生成や暗号鍵の生成をドキュメント保護プログラム 4 1 1 が行う場合を示したが、これらの処理はアクセスコントロールサーバ 4 0 4 や不図示のサーバなどで行っても良い。

また、配布者端末 4 0 1 とアクセスコントロールサーバ 4 0 4 との間が専用回線ではなくネットワーク網を介して接続されており、暗号鍵など送信する際に盗聴される懸念がある場合には、SSL (Secure Socket Layer) を用いて通信を行えばよい。

【0 1 5 1】

ドキュメント保護プログラム 4 1 1 がアクセスコントロールサーバ 4 0 4 と通信する際のプロトコルは、どのようなものを用いてもよい。例えば、分散オブジェクト環境を導入し、Java (R) RMI (Remote Method Invocation) や SOAP (Simple Object Access Protocol) をベースとして情報を送受信するようにしても良い。その場合、アクセスコントロールサーバ 4 0 4 は、例えば register(String docId, byte[] key, byte[] acl) のようなメソッドを実装するようにしてもよい。SOAP であれば、HTTPS の上で SOAP プロトコルをやりとりし、RMI であれば SSL ベースの SocketFactory を用いて RMI を実行するようにすれば、ネットワーク上でのセキュリティを確保することができる。

【0 1 5 2】

次に、ドキュメント印刷プログラム 4 2 1 が保護ドキュメントを印刷する際の動作について説明する。図 2 0 に、ドキュメント印刷プログラム 4 2 1 及びアク

セスコントロールサーバ 4 0 4 の動作の流れを示す。

ドキュメント印刷プログラム 4 2 1 は、ユーザ端末 4 0 2 の入力装置におけるユーザの入力操作によって保護ドキュメントとユーザ名とパスワードとを取得すると、保護ドキュメントに添付されているドキュメント ID を取得する。

そして、ユーザ名とパスワードとドキュメント ID とアクセスタイプ（ユーザが要求する処理を示す情報。ここでは、保護ドキュメントを印刷しようとするので、“print ” となる。）とをアクセスコントロールサーバ 4 0 4 へ送信して、アクセス権限があるか否かのチェックを要求する。

【 0 1 5 3 】

アクセスコントロールサーバ 4 0 4 は、ドキュメント印刷プログラム 4 2 1 からユーザ名とパスワードとドキュメント ID とアクセスタイプとを取得すると、ユーザデータベース 4 4 1 に登録されている情報を参照し、ユーザ認証を行う。

換言すると、アクセスコントロールサーバ 4 0 4 は、ユーザデータベース 4 4 1 に登録されている情報を参照し、ドキュメント印刷プログラム 4 2 1 から取得した情報に含まれるユーザ名とパスワードとの組と一致するものが、ユーザデータベース 4 4 1 に登録されているか否かを判断する。

【 0 1 5 4 】

ユーザ認証に失敗した場合（換言すると、ドキュメント印刷プログラム 4 2 1 から受け渡された情報に含まれるユーザ名とパスワードとを組としたものがユーザデータベース 4 4 1 に登録されていない場合）、アクセスコントロールサーバ 4 4 4 は、許可情報を「不許可」としてユーザ端末 4 0 2 へ送信し、ドキュメント印刷プログラム 4 2 1 へ受け渡す。なお、この場合は「エラー」とした許可情報をドキュメント印刷プログラム 4 2 1 へ受け渡すようにしてもよい。

【 0 1 5 5 】

一方、ユーザ認証に成功した場合、アクセスコントロールサーバ 4 0 4 は、セキュリティ属性データベース 4 4 3 に登録されているレコードのうち、ドキュメント印刷プログラム 4 2 1 から取得した情報に含まれるドキュメント ID に関するレコードを読み出す。また、アクセスコントロールサーバ 4 0 4 は、ユーザデータベース 4 4 1 からユーザの「階級」及び「部門」を取得する。

【0 1 5 6】

アクセスコントロールサーバ 4 0 4 は、読み出したレコードに基づいてドキュメントファイルに設定されているセキュリティ属性（すなわち、機密レベル及びカテゴリ）を取得する。そして、自身が記録保持しているセキュリティポリシーとレコードから読み出したセキュリティ属性に基づいて、ユーザがドキュメントに対してアクセスタイプで示される処理を行う場合の可否を示す許可情報とユーザがドキュメントを印刷する際の印刷要件を取得する。

【0 1 5 7】

ユーザにドキュメントファイルを印刷する権限がある場合は、セキュリティポリシーとして設定されている許可情報は「許可」であるため、アクセスコントロールサーバ 4 0 4 は、レコードに格納されていた暗号鍵と印刷要件とを許可情報とともにユーザ端末 4 0 2 へ送信して、ドキュメント印刷プログラム 4 2 1 に受け渡す。

【0 1 5 8】

一方、ユーザにドキュメントファイルを印刷する権限がない場合は、セキュリティポリシーとして設定されている許可情報は「不許可」であるため、アクセスコントロールサーバ 4 0 4 は、許可情報のみをユーザ端末 4 0 2 へ送信してドキュメント印刷プログラムに受け渡す。

また、ドキュメント印刷プログラム 4 2 1 は、許可情報と共に取得した印刷要件を満足するようにプリンタドライバを設定し（例えば、P A C が指定されていれば機密印刷モードに設定する）、プリンタ 4 0 3 にドキュメントファイルの印刷処理を実行させる。

なお、必要があれば、表示装置にメッセージを表示するなどして、印刷パラメータの設定をユーザに要求するようにしてもよい。

【0 1 5 9】

アクセスコントロールサーバ 4 0 4 から取得した印刷要件を満足する印刷をプリンタ 4 0 3 では実行できない場合、換言すると、プリンタ 4 0 3 がセキュリティポリシーとして設定されていた印刷要件を満たす機能を備えていない場合には、その旨を示すメッセージを表示装置に表示させるなどしてユーザに通知し、印

刷は行わずに処理を終了する。

【0 1 6 0】

以上の動作によって、ユーザごとに異なるアクセス権や印刷要件を設定することが可能となる。また、上記のように、サーバ側でドキュメントファイルに対するアクセス権を判断するシステム構成においては、アクセスコントロールサーバ 4 0 4 に登録されているセキュリティポリシーを配布者端末 4 0 1 やアクセスコントロールサーバ 4 0 4 における入力操作によって変更できるようにしてもよく、この場合には、保護ドキュメントを配布したあとで印刷要件を変更したりすることが可能となる。

例えば、既に配布した保護ドキュメントに対するアクセス権限を新たなユーザに設定したり、特定のユーザに対して印刷要件を追加することなどが可能となる。

【0 1 6 1】

なお、ドキュメントファイルを印刷する際に、ドキュメント印刷プログラム 4 2 1 が必ずアクセスコントロールサーバ 4 0 4 に対してセキュリティポリシーを問い合わせる方式とすると、ユーザ数の増加に伴いアクセスコントロールサーバ 4 の情報処理量が増え、負担が大きくなってしまう。

このため、アクセスコントロールサーバ 4 0 4 の機能の一部をドキュメント印刷プログラム 4 2 1 に移行してもよい。

【0 1 6 2】

例えば、ドキュメント印刷プログラム 4 2 1 は、ユーザ認証を行った上で、ドキュメント ID をアクセスコントロールサーバ 4 0 4 へ受け渡すと、セキュリティポリシーと暗号鍵とセキュリティ属性とをアクセスコントロールサーバ 4 0 4 から取得し、これを基に許可情報や印刷要件を判断して処理するようにしてもよい。

このようにすれば、アクセスコントロールサーバ 4 0 4 の情報処理量を減らし、システム動作上の負担を軽減できる。この場合は、セキュリティポリシーに基づいた判断をドキュメント印刷プログラム 4 2 1 が行うため、ドキュメントにセキュリティ属性を添付した後に暗号化して暗号化ドキュメントとし、ドキュメン

ト ID を添付して保護ドキュメントとすることが好ましい。これにより、セキュリティ属性をアクセスコントロールサーバ 4 0 4 で管理する必要がなくなり、システム動作上のアクセスコントロールサーバ 4 0 4 の負担をさらに軽減できる。

【 0 1 6 3 】

なお、本実施形態にかかるドキュメント保護・印刷システムが上記のような手法でドキュメントファイルを保護していることを知っている者は、ドキュメント印刷プログラム 4 2 1 に成りすますプログラムをコンピュータ端末に実行させて暗号鍵を不正に入手し、保護ドキュメントを復号化することも可能ではある。この場合は、セキュリティポリシーとして設定されている印刷要件を強制されることなく、保護ドキュメントを印刷できてしまうこととなる。

【 0 1 6 4 】

このため、単に暗号鍵のみを用いてドキュメントファイルを暗号化するのではなく、ドキュメント保護プログラム 4 1 1 の内部に埋め込まれた秘密鍵と暗号鍵とを合わせたもの（排他的論理和を取ったもの）でドキュメントファイルを暗号化することが好ましい。

この場合は、ドキュメント印刷プログラム 4 2 1 にも同一の秘密鍵を埋め込んでおくことで、配布者が設定した印刷要件を印刷時に強制するドキュメント印刷プログラム 4 2 1 のみが、保護ドキュメントを復号化して印刷することが可能となる。

【 0 1 6 5 】

また、本実施形態においては、ドキュメント印刷プログラム 4 2 1 は、ドキュメントファイルの印刷に関する処理のみを行っているが、ドキュメント印刷プログラム 4 2 1 は、ドキュメントファイルの内容をユーザに提示したり、ドキュメントファイルを編集する機能を備えていても良い。例えば、Adobe Acrobat の plug-in としてこの機能を実現することが可能である。

【 0 1 6 6 】

このように、本実施形態にかかるドキュメント保護・印刷システムによれば、予めセキュリティポリシーとして設定されている印刷要件をドキュメントを印刷する際に強制することができる。

【 0 1 6 7 】

図 2 1 に、上記各実施形態において適用されるプリンタが備えるセキュリティ機能の一部を示す。これらについて第 4 の実施形態におけるシステム構成を例として具体的に説明する。

まず、印刷要件として P A C が設定されている場合のドキュメント印刷プログラム 4 2 1 の動作について説明する。P A C が設定されている場合のドキュメント印刷プログラム 4 2 1 の動作を図 2 2 に示す。

(1) ドキュメント印刷プログラム 4 2 1 は P A C が設定されているドキュメントファイルを印刷する際には、図 2 3 に示すように、プリントダイアログを表示させた後に個人識別番号 (Personal Identification Number : P I N) を入力するダイアログをユーザ端末 4 0 2 の表示装置に表示させ、ユーザに P I N の入力を要求する。

(2) ユーザ端末 4 0 2 の入力装置を用いてユーザが P I N を入力すると、ドキュメント印刷プログラム 4 2 1 は、これをプリンタドライバに設定し、印刷を指示する。

プリンタドライバは、ドキュメントから Postscript などの P D L (Page Description Language) で記述された印刷データ (P D L データ) を生成し、印刷部数や出力トレイなどの印刷ジョブ情報を記述した P J L (Print Job Language) データを P D L データの先頭に付加する。プリンタドライバはさらに P J L データの一部として P I N を付加し、その P J L データ付き P D L データをプリンタ 4 0 3 に送る。

プリンタ 4 0 3 は、P J L データ付き P D L データを受け取ると P J L データの内容を参照し、機密印刷用の P I N が含まれている場合は印刷出力せずにプリンタ 3 内部の記憶装置 (HDD など) に P J L データ付き P D L データを保存する。ユーザが P I N をプリンタ 4 0 3 のオペレーションパネルを介して入力すると、プリンタ 4 0 3 は入力された P I N を P J L データに含まれる P I N と照合し、一致すれば P J L データに含まれていた印刷ジョブ条件 (部数、トレイなど) を適用しながら P D L データに従って印刷出力する。

(3) プリンタドライバに P I N が設定できない、すなわち、プリンタ 4 0 3

が機密印刷をサポートしていない場合には、機密印刷をサポートしている別のプリンタを選択するようにユーザに通知し、ドキュメントを印刷せずに処理を終了する。

【 0 1 6 8 】

このようにすることで、印刷実行後、プリンタ 4 0 3 のオペレーションパネルにおいて印刷実行前に入力したものと同一の P I N が入力されるまでドキュメントのプリントアウトがプリンタ 4 0 3 から出力されなくなる。このため、ドキュメントのプリントアウトがプリンタ 4 0 3 に不用意に放置されることがなくなり、プリントアウトによるドキュメントの漏洩を防止することが可能となる。

さらに、ネットワーク上を流れるプリントデータを盗聴されないようにプリンタ 4 0 3 とやりとりを S S L で保護してもよい。

【 0 1 6 9 】

また、ドキュメント印刷プログラム 4 2 1 を Windows (R) Domain のユーザ管理と連動させて、ユーザに対して P I N の入力を要求しないようにしてもよい。例えば、P I N をユーザに入力させるのではなく、Windows (R) Domain から現在ログオン中のユーザ I D を取得し、プリントデータとともにユーザ I D をプリンタ 4 0 3 へ送付するようにする。プリンタ 4 0 3 は、オペレーションパネルでユーザからのパスワード入力を受け、そのユーザ I D とパスワードとで Windows (R) Domain のユーザ認証機構を用いてユーザ認証を行い、成功すればプリントアウトするようにしても良い。Windows (R) Domain に限定されず、予め導入されているユーザ管理と連動させることで、ユーザにとって面倒な P I N 入力の手間を削減できる。

【 0 1 7 0 】

次に、印刷要件として E B C が設定されている場合のドキュメント印刷プログラム 4 2 1 の動作について説明する。

(1) ドキュメント印刷プログラム 2 1 は、E B C が設定されているドキュメントを印刷する際にドキュメント I D を示すバーコード画像データ（又は、二次元コード）のデータを生成する。

(2) ドキュメント印刷プログラム 4 2 1 は、生成したバーコード画像データ

をスタンプ画像としてプリンタドライバにセットし、プリンタ 4 0 3 に印刷を指示する。

(3) プリンタドライバに E B C が設定できない、すなわち、プリンタ 3 がスタンプ機能をサポートしていない場合は、スタンプ機能をサポートしている他のプリンタを選択するようにユーザに通知し、印刷を行わずに処理を終了する。

【 0 1 7 1 】

このようにすることで、ドキュメントのプリントアウトの各ページにはバーコードが印刷されるため、このバーコードを識別できる複写機、ファックス、スキヤナのみがバーコードをデコードすることでドキュメント I D を取得し、そのドキュメント I D を基にアクセスコントロールサーバ 4 0 4 でハードコピー、画像読み取り、ファックス送信などが許可されているか否かを判断することが可能となる。これにより、紙文書まで一貫したセキュリティ確保が可能となる。

【 0 1 7 2 】

次に、印刷要件として B D P が設定されている場合のドキュメント印刷プログラム 4 2 1 の動作について説明する。

(1) ドキュメント印刷プログラム 4 2 1 は、B D P が設定されているドキュメントを印刷する際に、印刷を要求しているユーザ名と印刷日時とを文字列として取得する（例えば、Ichiro, 2002/08/04 23:47:10）。

(2) ドキュメント印刷プログラム 4 2 1 は、ドキュメントのプリントアウトを複写機で複写した際に、生成した文字列が浮き上がるように地紋画像を生成する。

(3) ドキュメント印刷プログラム 4 2 1 は、生成した地紋画像をスタンプとしてプリンタドライバにセットし、プリンタ 4 0 3 にドキュメントの印刷を指示する。

(4) プリンタドライバに B D P が設定できない場合、すなわちプリンタ 4 0 3 が地紋印刷をサポートしていない場合には、地紋印刷をサポートしている別のプリンタを選択するようにユーザに通知し、印刷を行わずに処理を終了する。

【 0 1 7 3 】

このようにすることで、ドキュメントのプリントアウトの各ページには、印刷

処理を実行したユーザ名と日時とが浮き出る地紋画像として印刷され、プリントアウトを複写機やスキャナ、ファックスで処理すると文字列が浮き出ることとなる。これ、E B Cをサポートしていない複写機を使用する場合などに有効であり、ドキュメントのプリントアウトを複写することによる情報漏洩に対して抑止力を有する。

【0 1 7 4】

次に、印刷要件としてS L Sが設定されている場合のドキュメント印刷プログラム 4 2 1 の動作について説明する。

(1) ドキュメント印刷プログラム 4 2 1 は、S L Sが設定されているドキュメントファイルを印刷する際に、予め用意された画像のうち、そのドキュメントの機密レベルに応じたもの（Top Secretならば「極秘」のマークなど）を選択する。

(2) 選択した画像のデータを、スタンプとしてプリンタドライバにセットし、プリンタ 4 0 3 に印刷を指示する。

(3) プリンタドライバにS L Sをセットできない場合、すなわち、プリンタ 4 0 3 がS L Sをサポートしていない場合には、ラベルスタンプをサポートしている別のプリンタを選択するようにユーザに通知し、印刷を行わずに処理を終了する。

【0 1 7 5】

このようにすることで、ドキュメントファイルのプリントアウトには、自動的に「極秘」や「マル秘」がスタンプとして印刷されるため、ドキュメントが機密文書であることが明らかとなる。すなわち、プリントアウトを所持する者に管理上の注意を喚起することができる。

【0 1 7 6】

上記の各例は、あくまでも印刷要件の一例であり、改ざん防止用の電子透かしを印刷するようにしたり、保護されているドキュメントは特殊な用紙に印刷する（印刷に使用する用紙トレイを特殊用紙のトレイに限定する）ようにしてもよい。

このように、プリンタ 4 0 3 がサポートする様々なセキュリティ機能を利用し

てセキュリティポリシーを設定することによって、プリンタ 4 0 3 のセキュリティ機能を無駄なく活用して、プリントアウトに至るまで一貫したセキュリティの確保が可能となる。これは他の実施形態のシステム構成においても同様である。

【 0 1 7 7 】

なお、上記各実施形態は、本発明の好適な実施の一例であり、本発明はこれらに限定されることはない。

例えば、上記各実施形態においては、配布者端末とユーザ端末とが別個の装置である場合を例に説明を行ったが、これらは同一の装置を共用するような構成であっても構わない。

また、上記各実施形態では、ドキュメント印刷プログラムが実装されたユーザ端末を、ユーザが直接操作する場合を例に説明を行ったが、これに限定されるものではない。例えば、ドキュメント印刷プログラムがサーバに実装されており、ユーザがユーザ端末を操作しネットワーク網を介してドキュメント印刷プログラムを実行させる構成であってもよい。

また、ユーザ認証の方法は、ユーザ名とパスワードとを用いる方法に限定されることはなく、スマートカードを用いた P K I ベースの認証方法を適用してもよい。

このように、本発明は様々な変形が可能である。

【 0 1 7 8 】

【発明の効果】

以上の説明によって明らかなように、本発明によれば、ユーザの権限に応じたアクセス制限を施した状態でドキュメントファイルを配布できるとともに、プリントアウトによるドキュメントの漏洩を防止したドキュメントファイルの印刷制御方法、ドキュメントファイル印刷制御システム、ドキュメントファイル印刷制御プログラム、ドキュメントファイル保護方法、ドキュメントファイル印刷方法、ドキュメントファイル保護プログラム、ドキュメントファイル印刷プログラム及びコンピュータ装置を提供できる。

【図面の簡単な説明】

【図 1】

本発明を好適に実施した第 1 の実施形態にかかるドキュメント保護・印刷システムの構成を示す図である。

【図 2】

第 1 の実施形態にかかるドキュメント保護プログラムの動作を示す図である。

【図 3】

第 1 の実施形態にかかるドキュメント印刷プログラムの動作を示す図である。

【図 4】

本発明を好適に実施した第 2 の実施形態にかかるドキュメント保護・印刷システムの構成を示す図である。

【図 5】

A C L の構成例を示す図である。

【図 6】

第 2 の実施形態にかかるドキュメント保護プログラムの動作を示す図である。

【図 7】

A C L データベースに記録される情報の構造例を示す図である。

【図 8】

第 2 の実施形態にかかるドキュメント印刷プログラム及びアクセスコントロールサーバの動作の流れを示す図である。

【図 9】

本発明を好適に実施した第 3 の実施形態にかかるドキュメント保護・印刷システムの構成を示す図である。

【図 1 0】

第 3 の実施形態にかかるドキュメント保護プログラム及びアクセスコントロールサーバの動作の流れを示す図である。

【図 1 1】

第 3 の実施形態にかかるドキュメント印刷プログラムの動作を示す図である。

【図 1 2】

第 3 の実施形態にかかるドキュメント印刷プログラム及びアクセスコントロールサーバの動作の流れを示す図である。

【図 13】

セキュリティポリシーの一例を示す図である。

【図 14】

本発明を好適に実施した第4の実施形態にかかるドキュメント保護・印刷システムの構成を示す図である。

【図 15】

セキュリティポリシーを電子データとした場合のデータ構造を示す図である。

【図 16】

セキュリティポリシーを電子データとして記述した例を示す図である。

【図 17】

ユーザデータベースに記録される情報の構造例を示す図である。

【図 18】

第4の実施形態にかかるドキュメント保護プログラムの処理を示す図である。

【図 19】

第4の実施形態にかかるドキュメント保護プログラム及びアクセスコントロールサーバの動作の流れを示す図である。

【図 20】

第4の実施形態にかかるドキュメント印刷プログラム及びアクセスコントロールサーバの動作の流れを示す図である。

【図 21】

プリンタが備えるセキュリティ機能の一例を示す図である。

【図 22】

PACが設定されたドキュメントを印刷する際の処理を示す図である。

【図 23】

PIN入力のダイアログを示す図である。

【符号の説明】

101、201、301、401 配布者端末

102、202、302、402 ユーザ端末

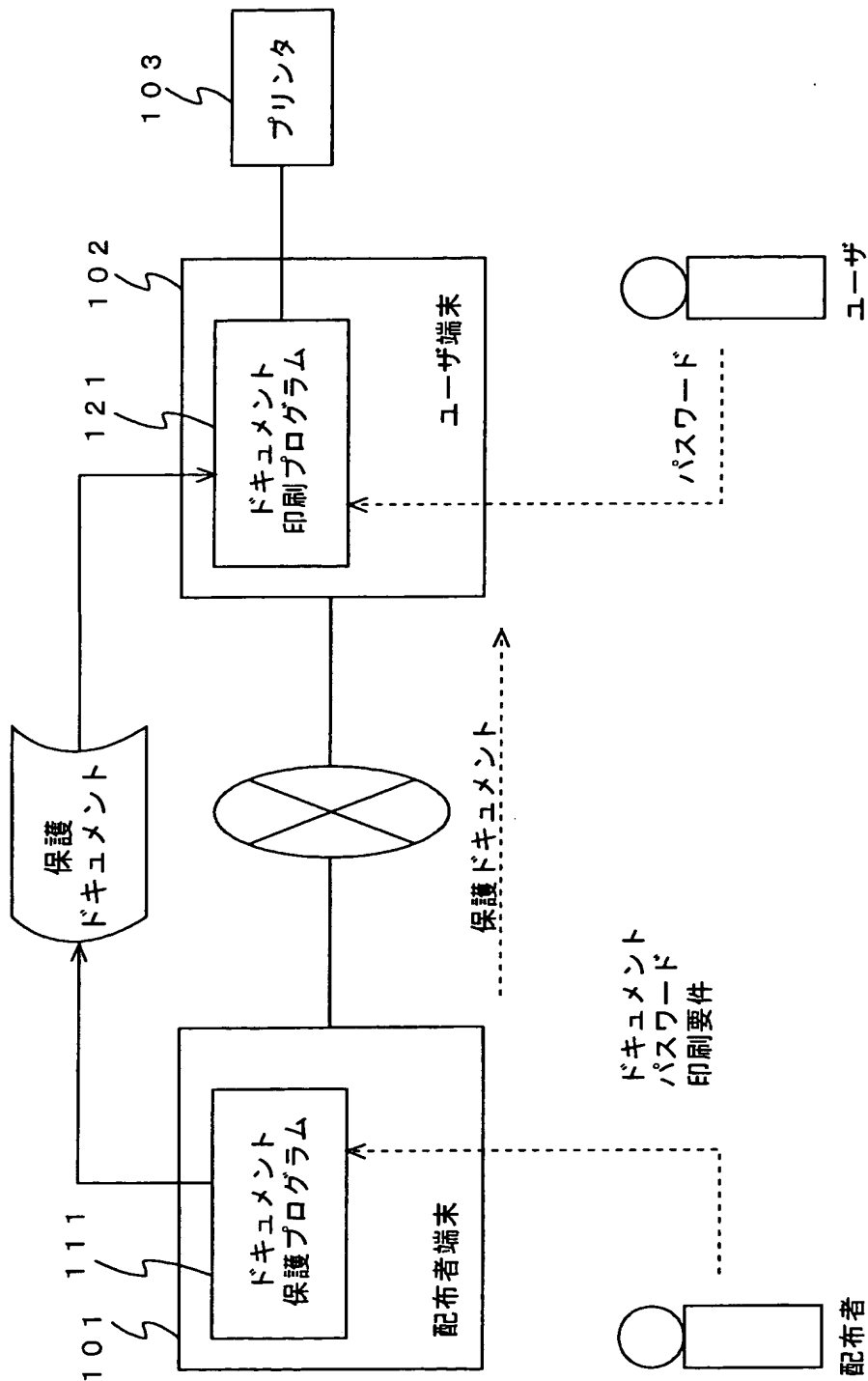
103、203、303、403 プリンタ

1 1 1、2 1 1、3 1 1、4 1 1 ドキュメント保護プログラム
1 2 1、2 2 1、3 2 1、4 2 1 ドキュメント印刷プログラム
2 0 4、3 0 4、4 0 4 アクセスコントロールサーバ
2 4 1、3 4 1、4 4 1 ユーザデータベース
2 4 2、3 4 2 A C L データベース
3 4 3、4 4 3 セキュリティ属性データベース

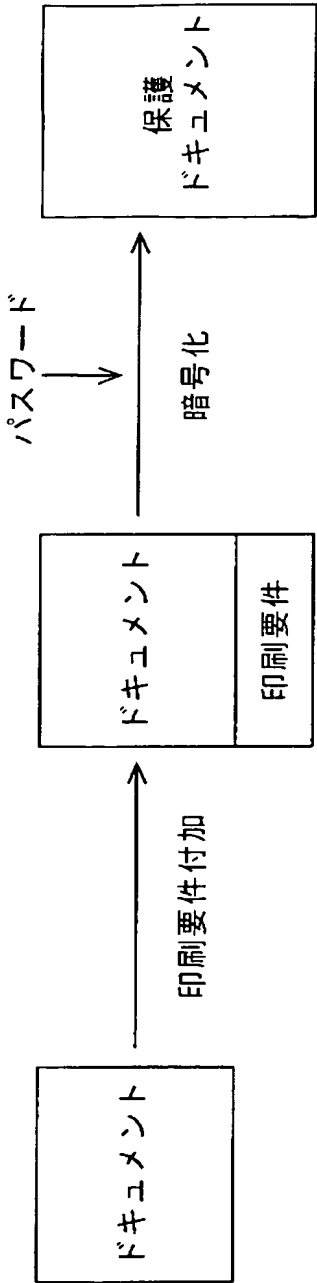
【書類名】

図面

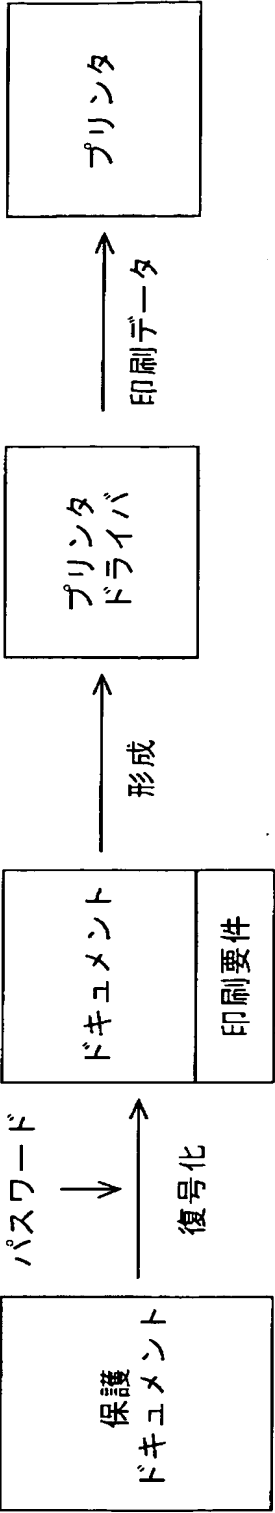
【図 1】



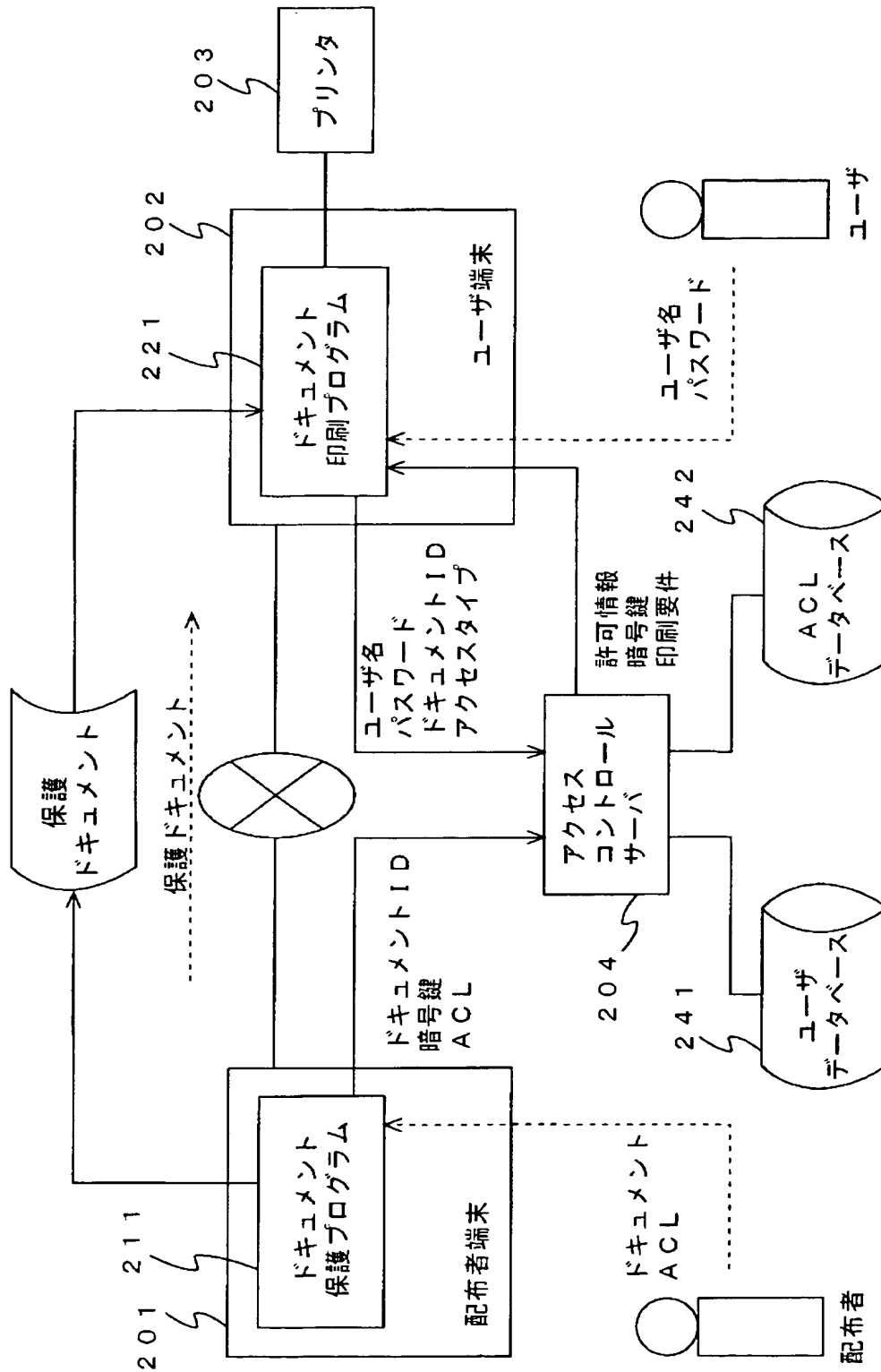
【図 2】



【図 3】



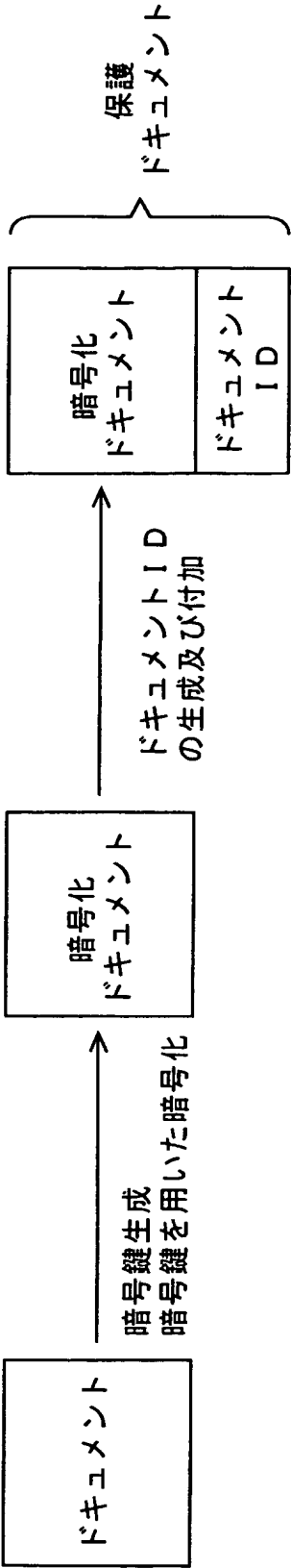
【図 4】



【図 5】

User name	Access type	Permission	Requirement
Ichiro	Read	Allowed	—
	Write	Denied	—
	Print	Allowed	PAC(Private Access)
			BDP(Background Dot Patten)
			EBC(Embedding BarCode)
	Hardcopy	Allowed	RAD(Record Audit Date)
Taro	Read	Allowed	—
	Write	Denied	—
	Print	Denied	—
	Hardcopy	Denied	—
⋮			

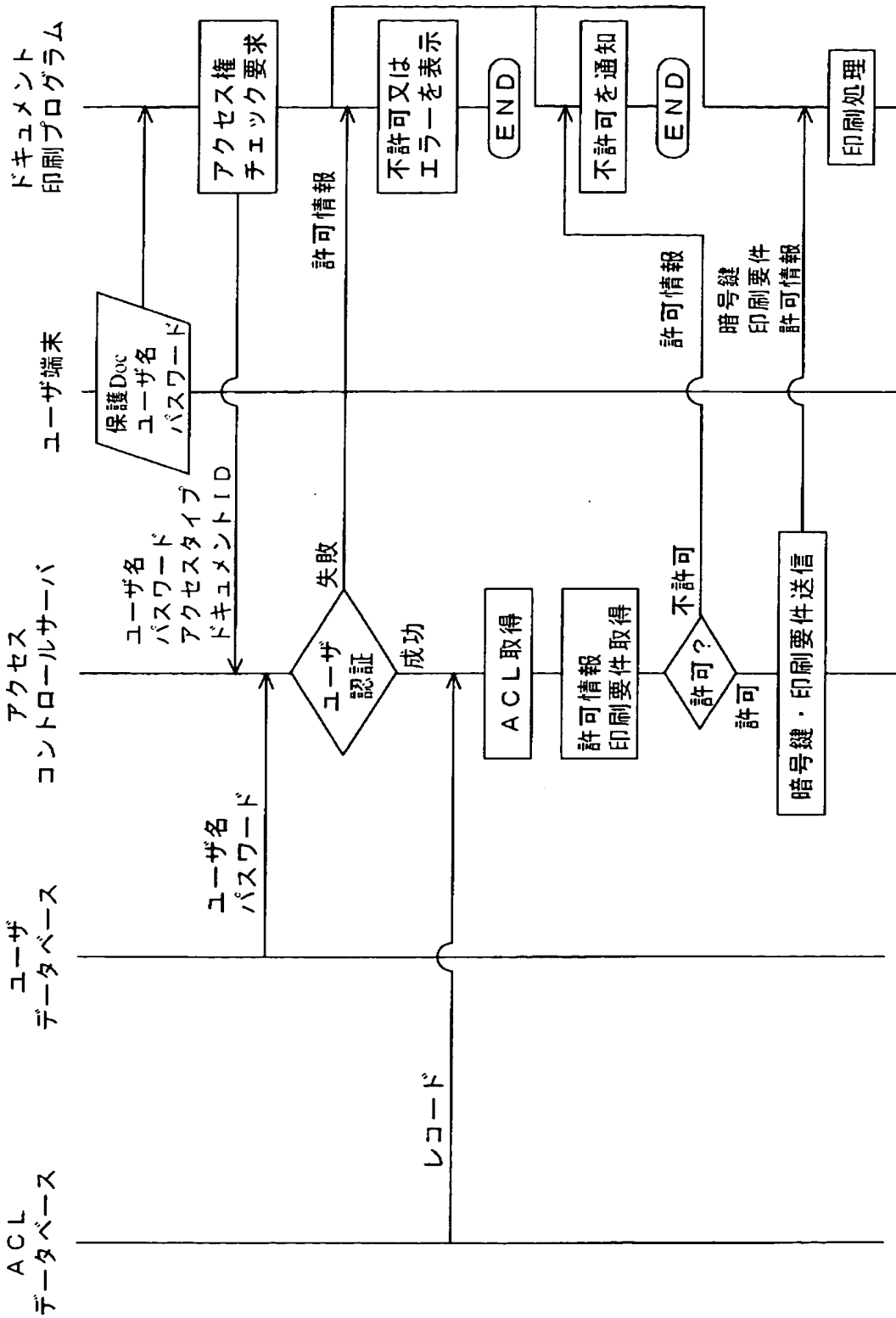
【図 6】



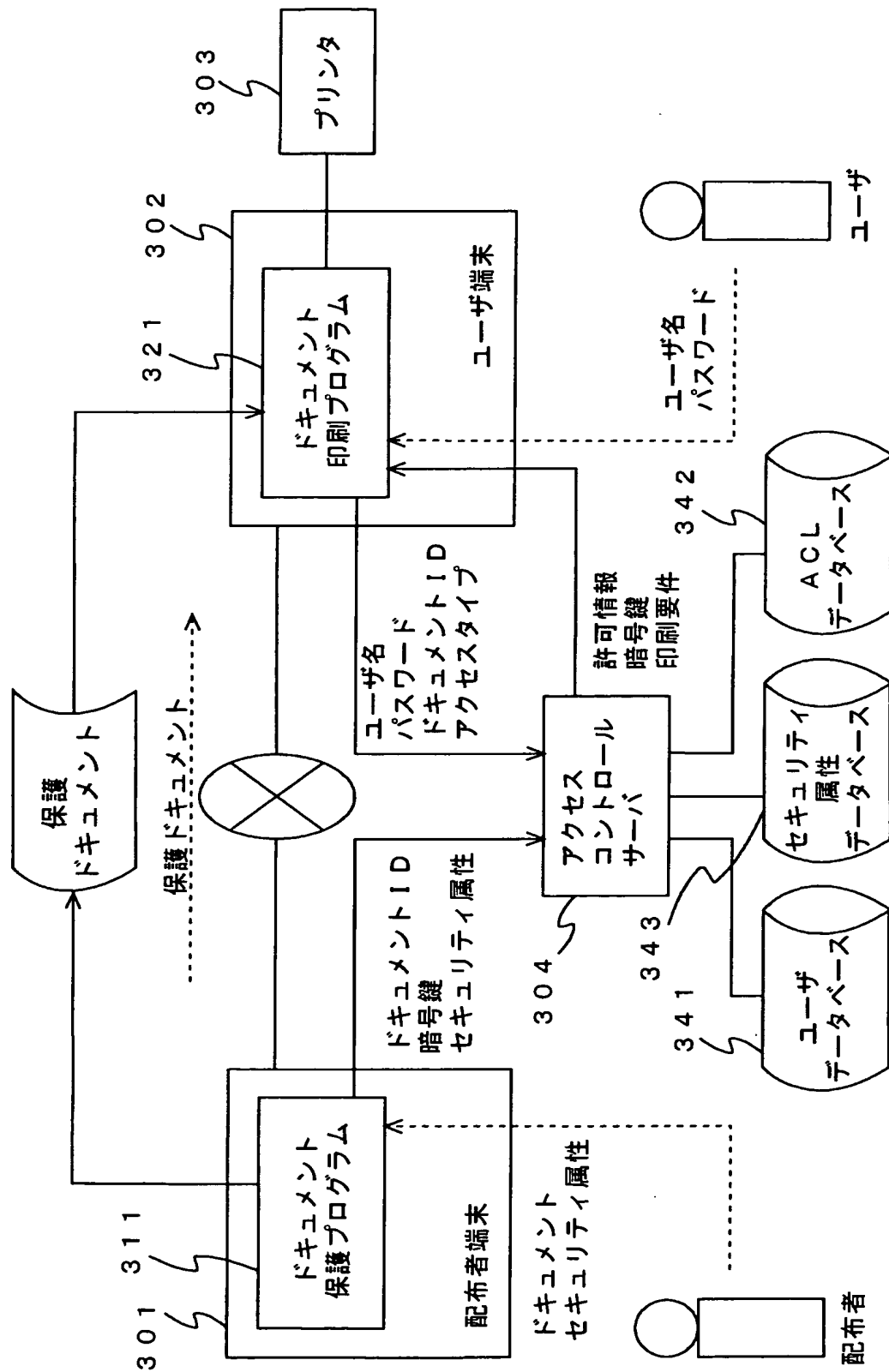
【図 7】

Document ID	Key	ACL
133.139.234.23.22.125.98.192	89FECA8D2B	(binary data)
133.139.234.23.22.125.99.105	A73C44DA59	(binary data)

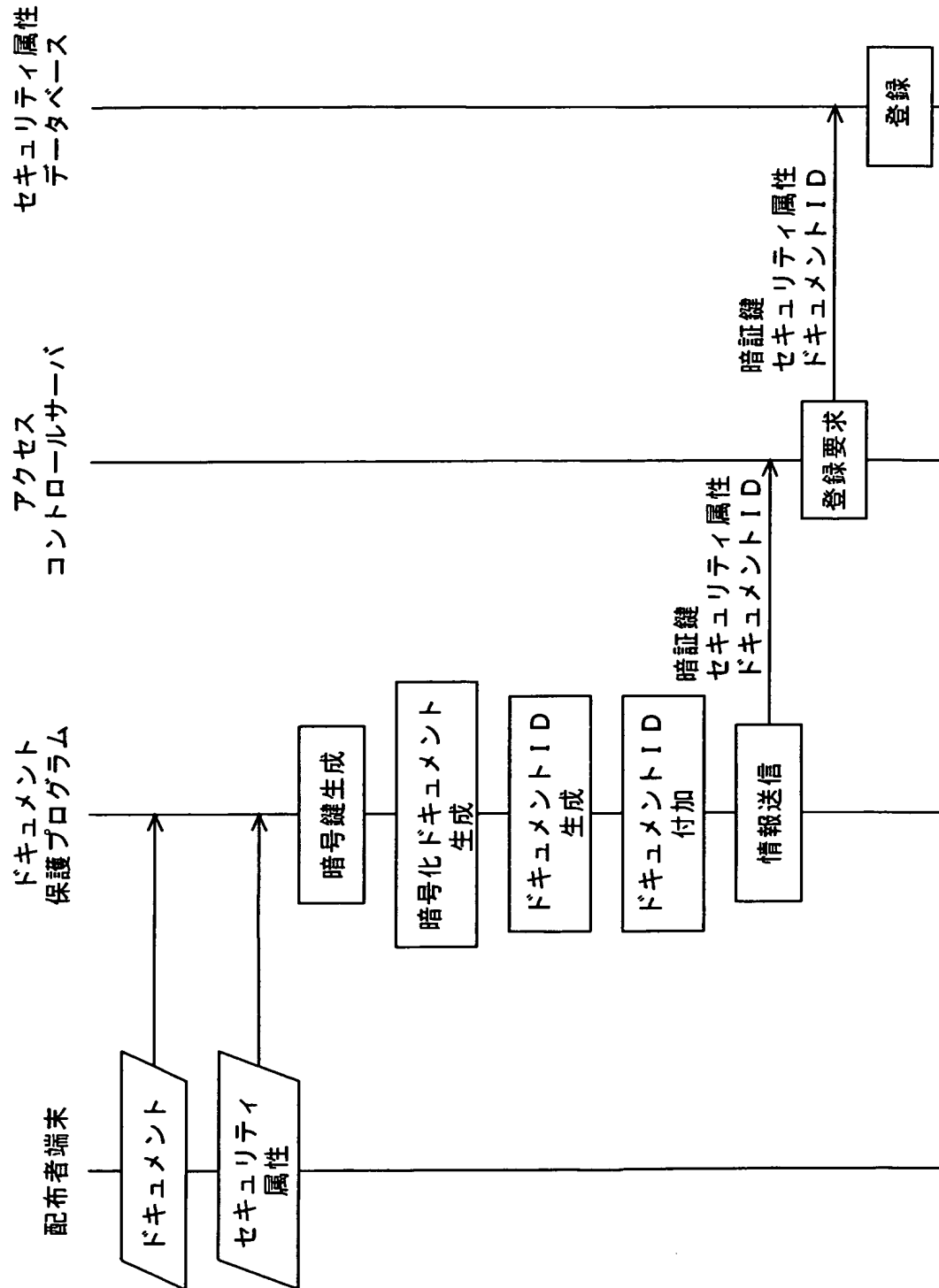
【図8】



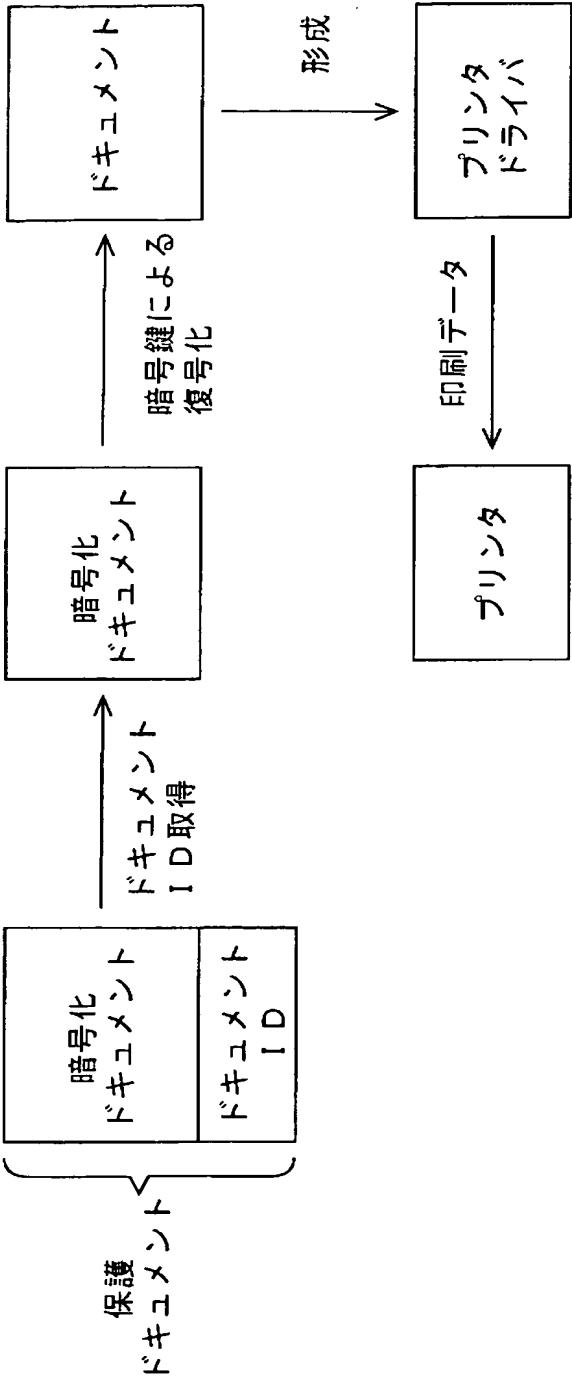
【図 9】



【図 10】



【図 11】



【図 13】

極秘文書について：

原則複写禁止（複写する際には管理責任者の許可を得なければならない。また、複写したことを記録しておかなければならない。プリントする際には複写禁止であることを示す透かしを入れなければならない。また、プリントしたことを記録しておかなければならない。

閲覧は関係者のみ許可

丸秘文書について：

複写は関係者のみ許可

プリントする際には丸秘文書であることを示すラベルを同時に印刷しなければならない。

閲覧は関係者のみ許可

社外秘文書について

社外へ送付する際には管理者の許可を得なければならない。

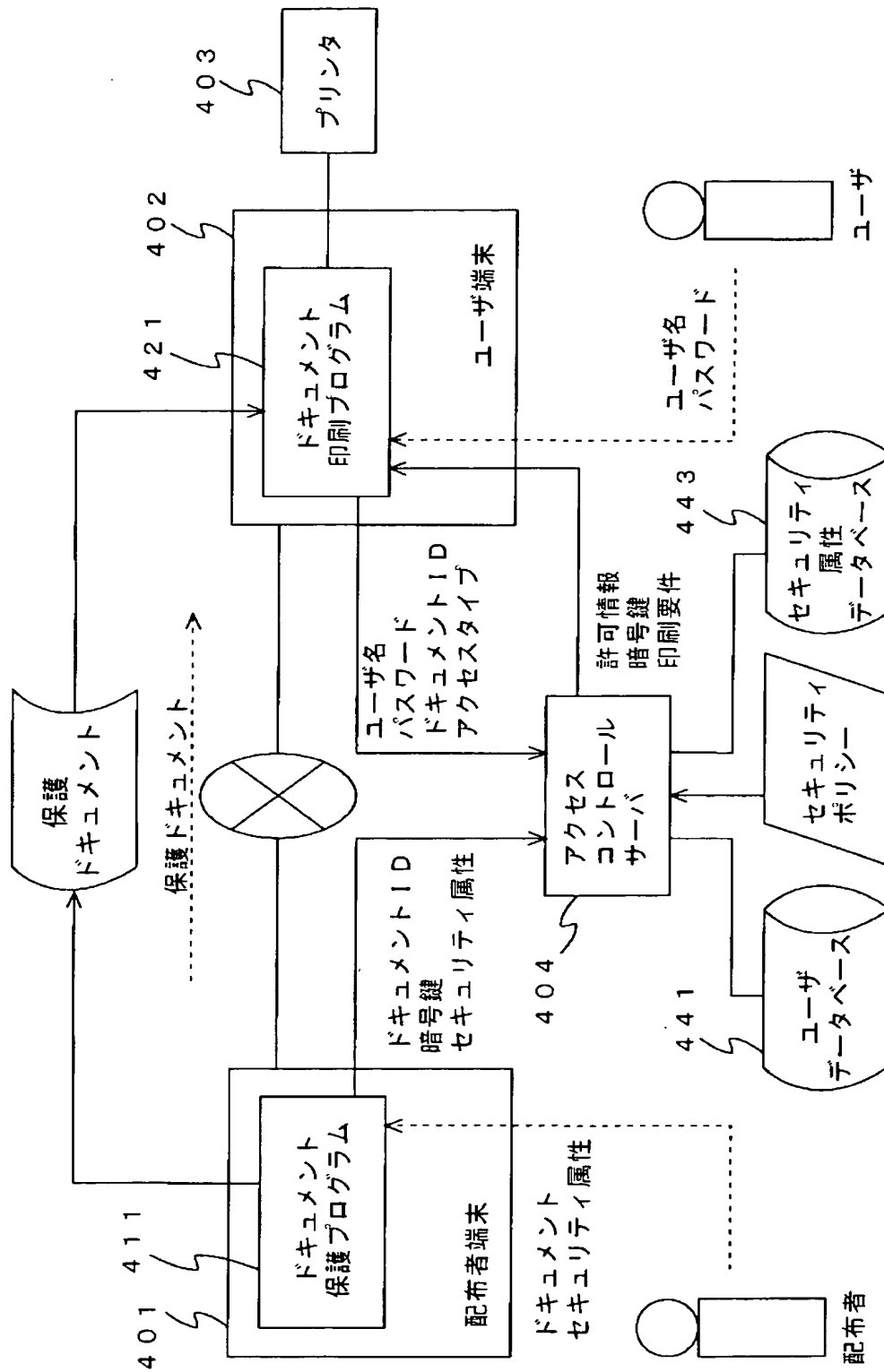
複写・プリント・閲覧は社内であれば許可不要

人事関連文書について

全て丸秘文書として扱う

・
・
・
・

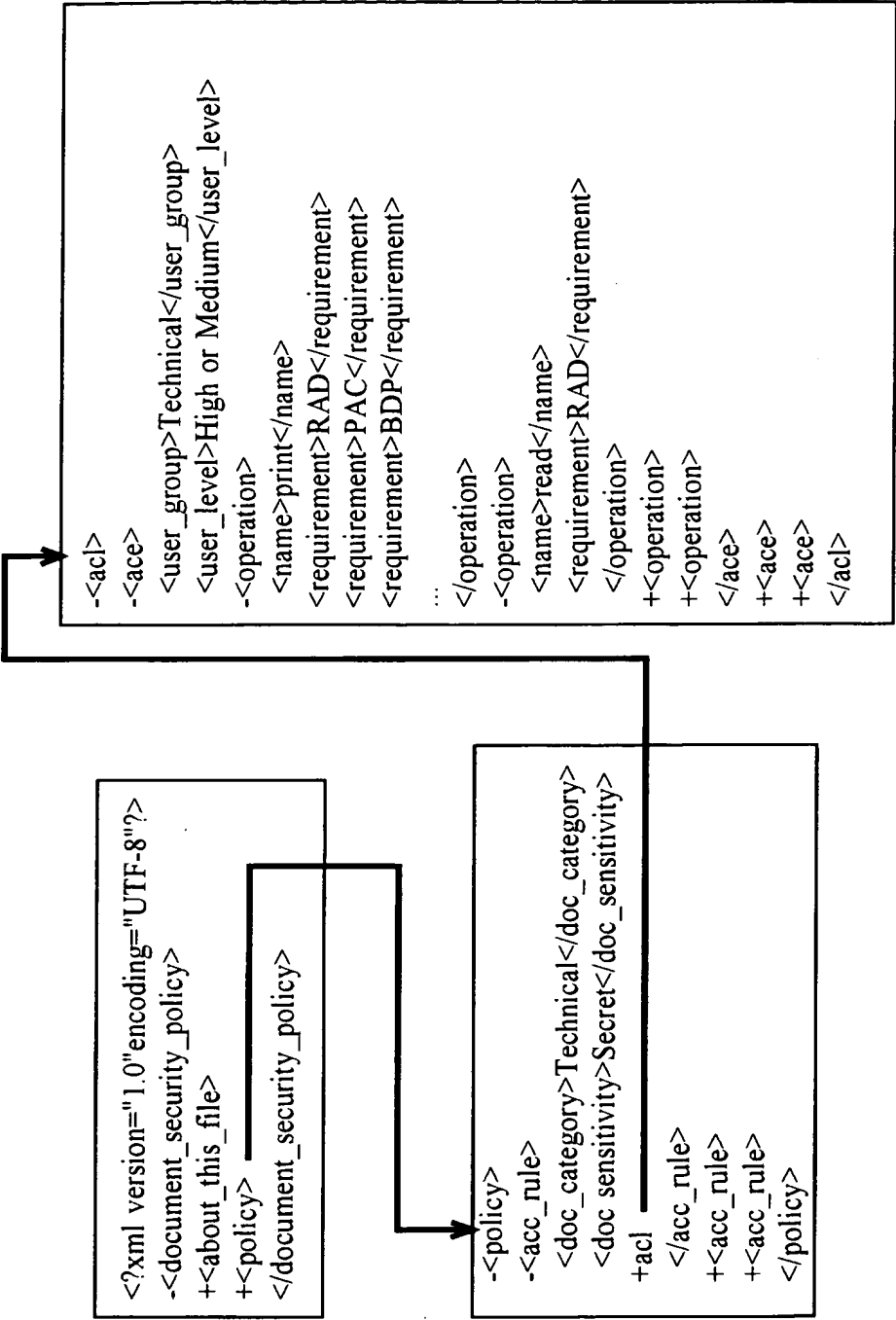
【図 14】



【図 1 5】

Document Type		User Type		Access Type	Permission	Requirement
Category	Sensitivity	Category	Level			
Technical	Secret	Technical	Medium High	Read	Allowed	RAD
				Print	Allowed	PAC BDP EBC RAD
				Hardcopy	Denied	
				...		
Technical	Top Secret	Technical	High	...		
				...		
				...		
Human Resource	Top Secret	Human Resource	High	Read	Allowed	RAD
				Print	Denied	
				Hardcopy	Denied	

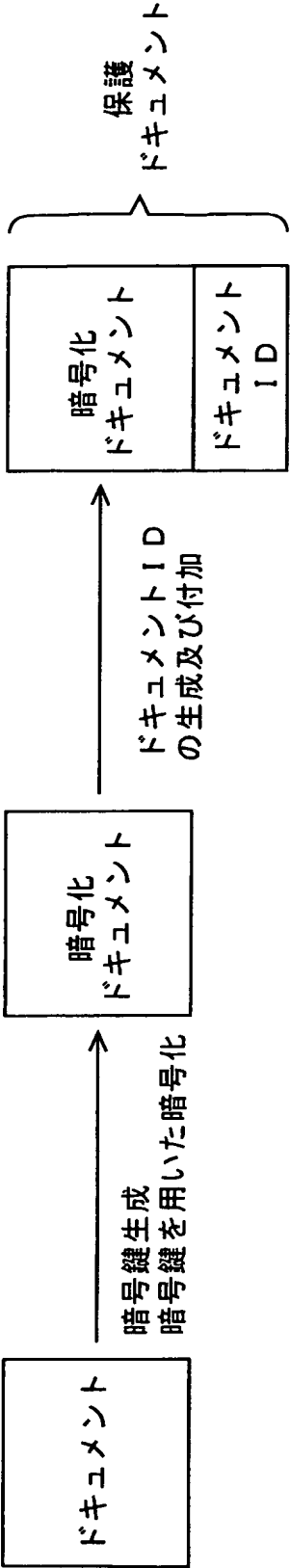
【図 1 6】



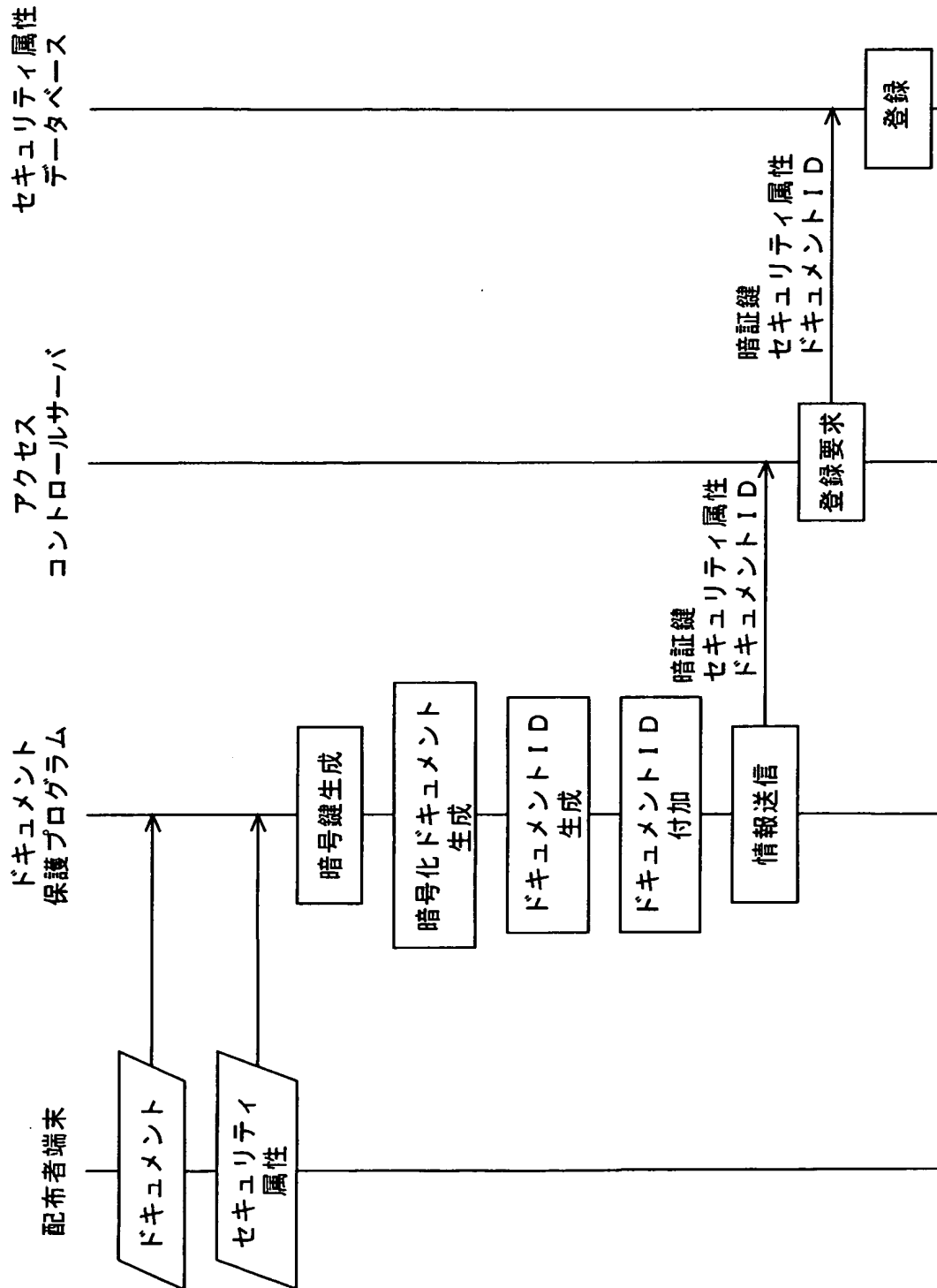
【図 1 7】

User name	Password	Category	Level
Ichiro	98q34rah	Technical	Medium
		General	Basic
Taro	Adoijoqer	Human Resource	Top Secret
		General	Basic
⋮			

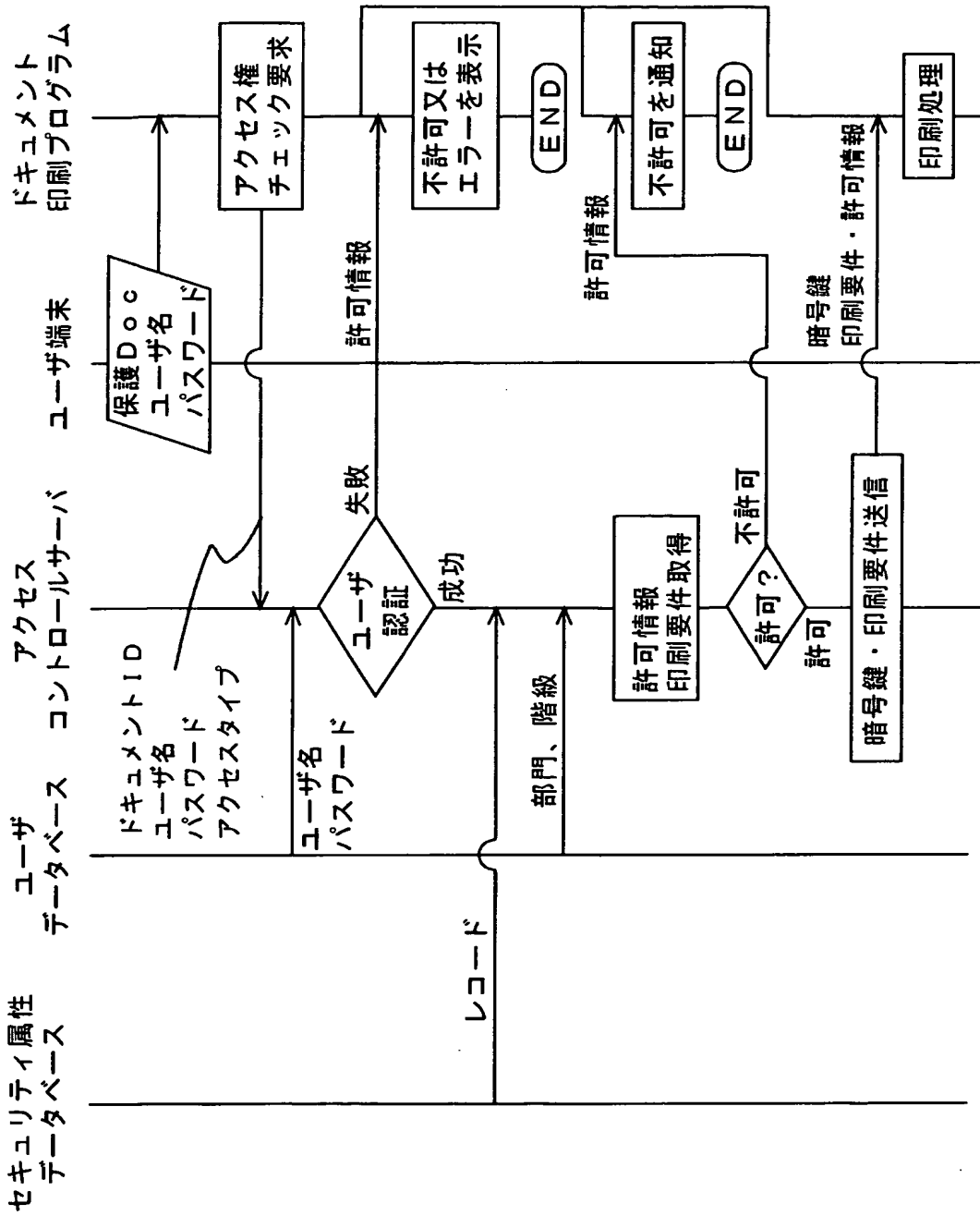
【図 1 8】



【図 19】



【図 20】

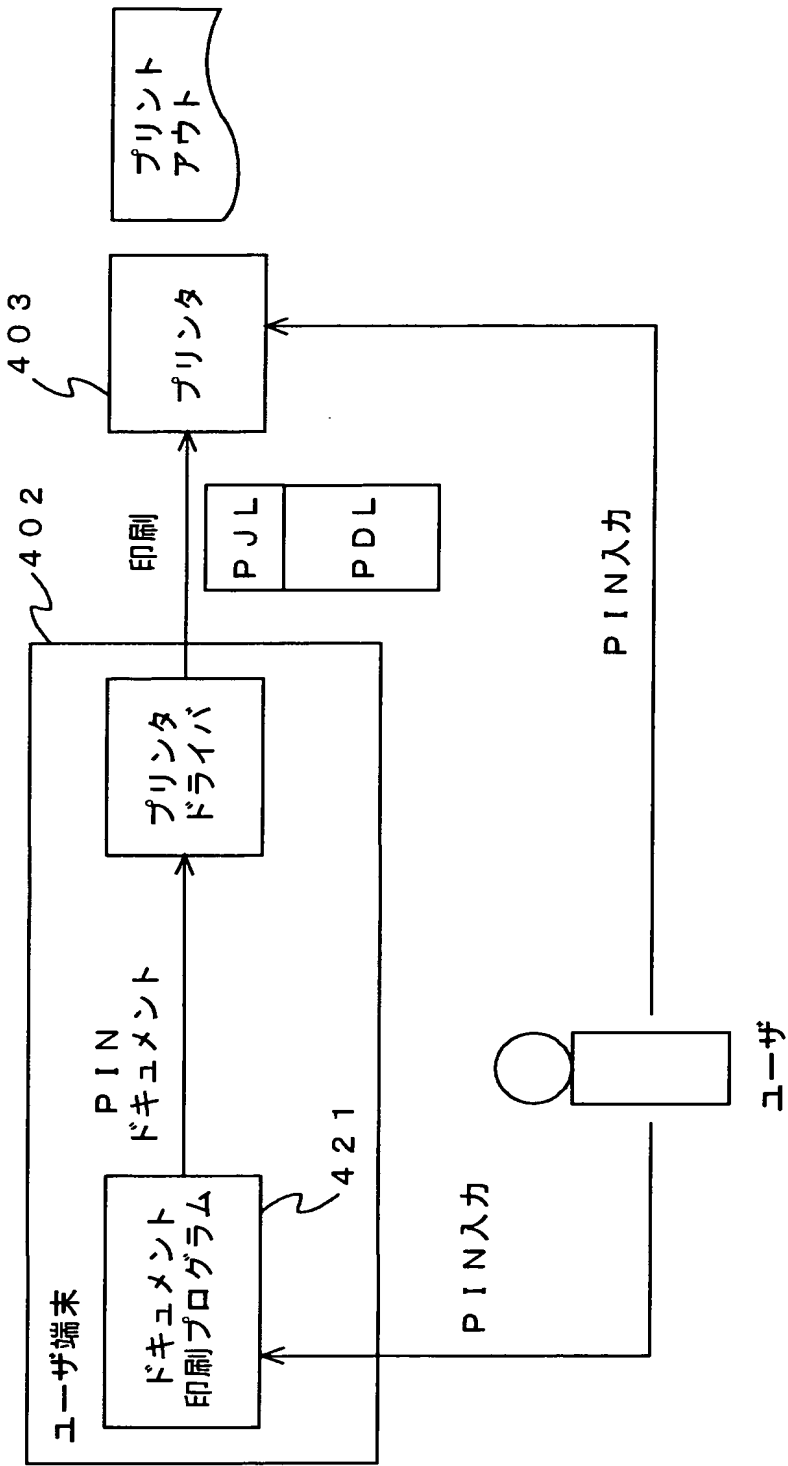


【図 21】

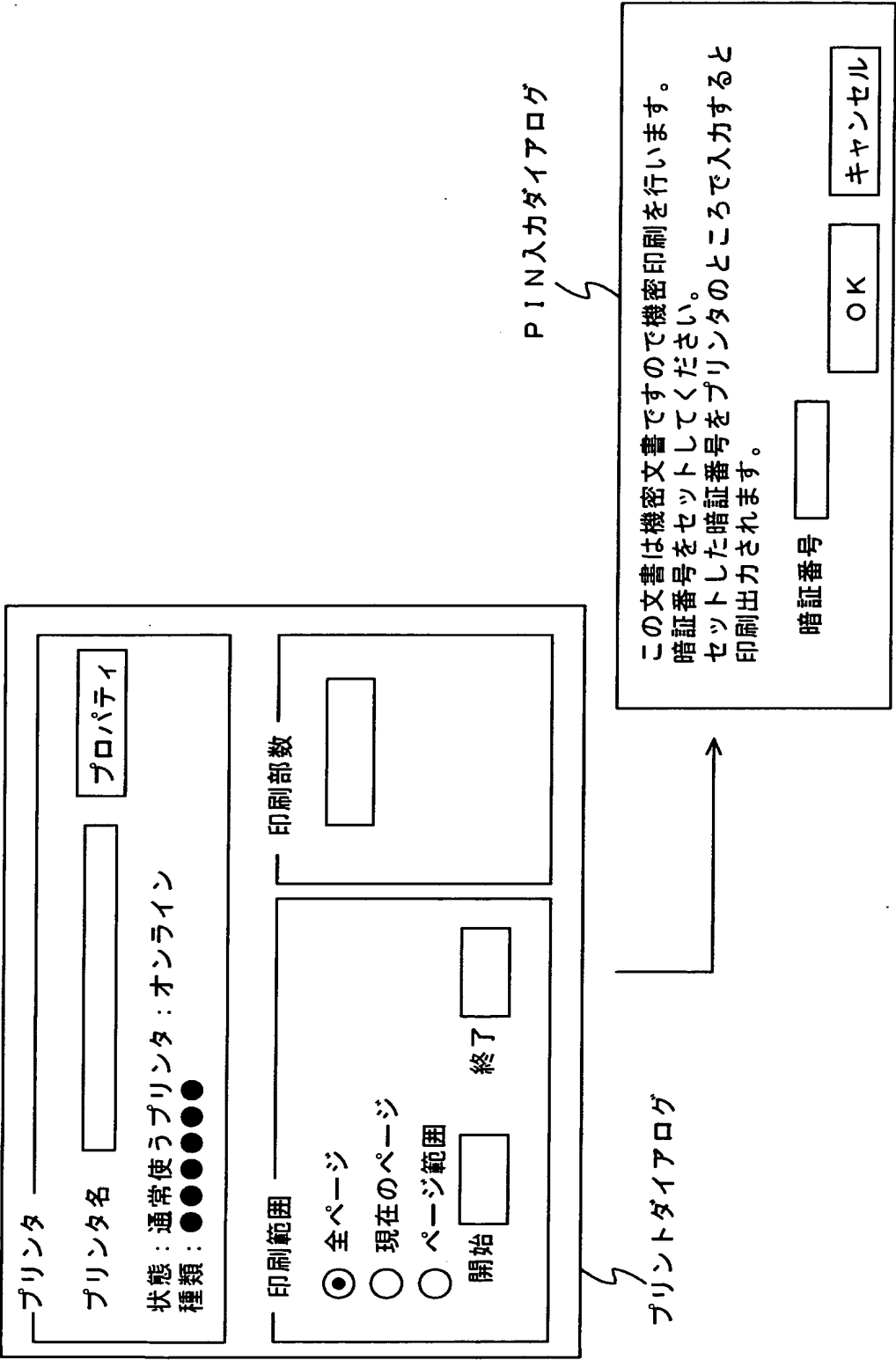
プリントセキュリティ機能

スタンプ機能	マル秘などのマークをスタンプやウォーターマークとしてページ内の任意の場所に重ねて印刷する機能。スタンプに使用することができるのは「秘」や「CONFIDENTIAL」などの文字列やビットマップ画像である。
地紋印刷機能	複写機で複写されると特定のイメージが浮き上がるようにコントロールした地紋画像を原稿に重ね合わせて印刷する機能。上記のスタンプ機能でスタンプとして指定する画像を地紋画像にすることで実現する手法が一般的である。
機密印刷機能	印刷を指示する際にプリンタドライバに P I N (Personal Identification Number) を指定すると、印刷した本人がプリンタのところへ行き、プリンタのオペレーションパネルでその P I N を入力しなければプリントアウトされない機能。

【図 22】



【図 23】



【書類名】 要約書

【要約】

【課題】 ユーザの権限に応じたアクセス制限を施した状態でドキュメントファイルを配布できるとともに、プリントアウトによるドキュメントの漏洩を防止したドキュメントファイルの印刷制御方法、ドキュメントファイル印刷制御システム、ドキュメントファイル印刷制御プログラム、ドキュメントファイル保護方法、ドキュメントファイル印刷方法、ドキュメントファイル保護プログラム、ドキュメントファイル印刷プログラム及びコンピュータ装置を提供する。

【解決手段】 ドキュメント保護プログラム 111 は、ドキュメントファイルに、該ドキュメントファイルの印刷要件を付与し、印刷要件を満たすことなくドキュメントファイルを印刷することを禁止することにより該ドキュメントファイルを保護し、ドキュメント印刷プログラム 121 は保護されたドキュメントファイルをプリンタ 3 を用いて印刷する際に、印刷要件を満たすように印刷処理を行う。

【選択図】 図 1

特願 2 0 0 2 - 2 9 9 7 1 2

出 願 人 履 歴 情 報

識別番号

[0 0 0 0 0 6 7 4 7]

1. 変更年月日 1 9 9 0 年 8 月 2 4 日
 [変更理由] 新規登録
 住 所 東京都大田区中馬込 1 丁目 3 番 6 号
 氏 名 株式会社リコー

2. 変更年月日 2 0 0 2 年 5 月 1 7 日
 [変更理由] 住所変更
 住 所 東京都大田区中馬込 1 丁目 3 番 6 号
 氏 名 株式会社リコー